ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Telnet et ftp sous Gnu/Linux

www.ofppt.info

OFPPT

DIRECTION RECHERCHE ET INGENIERIE DE FORMATION

SECTEUR NTIC

Sommaire

1.1. Principe

Le document décrit l'installation d'un service de transfert de fichiers, la configuration du service inetd et quelques premiers aspects touchant à la sécurité des services sous GNU/Linux.

Mots clés : Telnet, FTP, ssh, sftp, scp, TCP-Wrapper

1.2. Description et objectifs de la séquence

Vous devriez à la fin pouvoir :

- utiliser le service FTP du serveur à partir d'un client quelconque du réseau
- bénéficier du service ftp anonyme ou authentifié,
- pouvoir filtrer l'accès provenant de tout ou partie du réseau avec TCP-Wrapper.

1.3. Présentation des concepts importants

1) Telnet:

Telnet est un protocole qui permet l'émulation de terminal VTx à distance sur un serveur Unix/Linux.

2) FTP:

FTP est un protocole de communication qui permet le transfert de fichiers entre plusieurs machines.

3) Le daemon inetd:

Toute application fonctionnant sous TCP/IP est basée sur le modèle client/serveur. Par exemple quelqu'un se connectant via telnet à un hôte distant « active » chez l'hôte le service serveur telnetd.

Chaque serveur est sur une machine en attente d'une connexion sur un port particulier. Dans les premières versions d'Unix-TCP/IP chaque application (telnet, ftp,...) avait son propre serveur qui était lancé au démarrage de chaque machine comme un "daemon". Cette stratégie encombrait inutilement la table des processus (autant de serveurs que de services). Ces services sont dits fonctionnant en mode « autonome » ou « standalone ».

Le daemon INETD est un « super » serveur, à l'écoute sur plusieurs ports et qui se charge de recevoir les demandes de connexion de plusieurs clients (telnet, ftp,...) et de lancer le serveur correspondant à la demande. A son démarrage il consulte les fichiers:

- /etc/services qui contient la liste générale des services TCP/IP avec leur numéro de port et le protocole de transport associé.

- /etc/inetd.conf qui contient la liste des services activés sur une machine donnée

Dans les distributions récentes (Mandrake 10.x, RedHat 9.x...), inetd a été remplacé par xinetd. Le principe est très similaire, à la seule différence que, dans /etc/etc/xinetd.d, chaque service (telnet, ftp, pop3...) dispose de son propre fichier de configuration.

Certains services utilisables avec inetd ou xinetd comme telnet, ftp, pop3... sont difficilement sécurisables car les mots de passe transitent en clair sur le réseau. Ce problème sera vu ultérieurement avec les TPs sur la métrologie. Si ces services sont utilisables en l'état sur des petits réseaux isolés, il faudra éviter de les utiliser sur des réseaux reliés à Internet ou dans des environnements peu sûrs. Cependant, la tendance est au cryptage de ces services, grâce à SSL notamment. Il existe une version sécurisée de telnet, nommée telnet-ssl.

1.4. Extrait de /etc/services :

/etc/services :

```
ftp  21/tcp
telnet  23/tcp
smtp  25/tcp  mail
pop3  110/tcp  # Post Office
```

etc...

1.5. Extrait de /etc/inetd.conf

```
ftp      stream  tcp     nowait  root    /usr/sbin/ftpd          ftpd
#shell   stream  tcp     nowait  root    /usr/sbin/rshd          rshd
#login   stream  tcp     nowait  root    /usr/sbin/rlogind       rlogind
#exec    stream  tcp     nowait  root    /usr/sbin/rexecd        rexecd
```

Ici, il n'y a que le service ftp qui est activé par le serveur inetd. Les autres lignes sont en commentaires.

Ces services sont dits fonctionnant en mode « parallèle ».

1.6. Configuration avec xinetd

Le principe est similaire, à la différence que vous avez un fichier de configuration global "/etc/xinetd.conf", et un fichier de configuration par service, en général dans le répertoire "/etc/xinetd.d/".

```
#
# Le fichier xinetd.conf
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
```

```
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}

includedir /etc/xinetd.d
```

Le fichier /etc/xinetd.d/wu-ftpd

```
# default: on
# description: The wu-ftpd FTP server serves FTP connections. It uses \
#       normal, unencrypted usernames and passwords for authentication.
service ftp
{
        disable = no
        socket_type             = stream
        wait                    = no
        user                    = root
        server                  = /usr/sbin/in.ftpd
        server_args             = -l -a
        log_on_success          += DURATION USERID
        log_on_failure          += USERID
        nice                    = 10
}
```

Le paramètre "disable", permet d'activer/désactiver le service.

le programme "in.ftpd", indique bien que le service est pris en charge par TCPWrapper (C'est le in qui l'indique, sinon, le binaire s'appellerait ftpd).

Les commentaires en haut du fichier indiquent que ce service ne prend pas en charge l'encryptage des mots de passe.

1.7. TCP-Wrapper

TCP-Wrapper est un outil de sécurité réseau qui permet de contrôler les accès, les tentatives de connexion sur une machine donnée. Il permet à tout instant de savoir (par journalisation syslogd) qui essaie d'accéder sur un ordinateur mais également de filtrer les accès. On peut par exemple sur une machine A interdire les connexions telnet venant d'une machine B tout en autorisant les connexions FTP venant de cette même machine B.

Principe de fonctionnement:

Exemple: Si inetd reçoit une demande de connexion sur le port 23 il va lancer telnetd.

Tcpwrapper sert d'enveloppe. Il vient « s'intercaler » entre le daemon inetd et le serveur à démarrer. Quand une demande de service TCP/IP (en réalité TCP ou UDP) arrive sur un port donné, inetd va lancer TCPD (daemon correspondant à Tcpwrapper) au lieu d'activer directement le service demandé (telnetd, ftpd, pop3...).

Tcpd prend en charge la requête et met en place ses mécanismes de contrôle. Il peut par exemple vérifier que les accès depuis la machine cliente sont autorisés. Une fois le traitement

terminé il va (s'il y a autorisation) lancer son propre service in.telnetd, in.ftpd, in.imapd....

1.8. Eléments de configuration

Sous Linux, tcpd est installé par défaut. On peut voir en consultant le fichier /etc/inetd.conf comment inetd active tcpd.

1.8.1. Extrait de /etc/inetd.conf

```
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd  in.ftpd -l -a
telnet  stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
```

1.8.2. TCP Wrapper

L'administrateur réseau va pouvoir utiliser 2 fichiers: /etc/hosts.allow et /etc/hosts.deny pour filtrer les accès à sa machine.

/etc/hosts.deny: on indique dans ce fichier les services et les hôtes pour lesquels l'accès est interdit.

/etc/hosts.allow: on indique dans ce fichier les services et les hôtes pour lesquels l'accès est autorisé.

Exemple:

```
# Fichier /etc/hosts.deny
# interdit tous les accès ftp à la machine
in.ftpd:ALL

# Fichier /etc/hosts.allow
# autorise les accès ftp venant de cli1
in.ftpd :cli1.archinet.edu
```

TCP-Wrapper utilise l'algorithme suivant :

```
Si une règle est applicable dans hosts.allow, alors cette règle est
appliquée, sinon, Si une règle est applicable dans hosts.deny alors cette
règle est appliquée, sinon, l'accès est autorisé.
```

Ce mode de fonctionnement induit la stratégie de sécurité à adopter :

1. décrire toutes les règles pour les couples (services/clients) qui sont autorisés,
2. interdire systématiquement tout le reste. Mettre par défaut ALL:ALL dans hosts.deny.

Les tentatives d'accès depuis des machines extérieures sont toutes enregistrées dans des fichiers particuliers. Ces enregistrements sont effectués par le processus syslogd qui, à son démarrage, lit le fichier /etc/syslog.conf pour trouver dans quel(s) fichier(s) il doit enregistrer les différentes tentatives d'accès.

1.9. Extrait de /etc/syslog.conf

```
# Log anything (except mail) of level info or higher.
```

```
# Don't log private authentication messages

# The authpriv file has restricted access.
authpriv.*                                      /var/log/auth.log
auth,authpriv.none;                             /var/log/syslog
```

1.10. Extrait de /var/log/syslog

```
Feb  3 18:02:52 ns1 ftpd[1051]: FTP session closed
Feb  3 18:03:31 ns1 syslogd 1.3-3: restart.
Feb  3 18:07:34 ns1 in.ftpd[1057]: refused connect from cli1.archinet.edu
Feb  3 18:07:46 ns1 in.ftpd[1058]: connect from ns1.archinet.edu
Feb  3 18:10:57 ns1 login[1063]: LOGIN ON ttyp3 BY mlx FROM puce
```

Remarques:

La commande kill -HUP pid de sysklogd permet de redémarrer ce processus avec prise en compte des paramètres se trouvant dans /etc/syslog.conf. Il est aussi possible d'invoquer le script de lancement du service en lui passant l'argument restart : /etc/init.d/syslogd restart