Gestion automatique des accès extérieurs

■ Daniel GUENICHE, gueniche@labs.ploycnrs-gre.fr
CNRS, Grenoble

L'utilisation continue d'un serveur de messagerie abritant un millier de comptes actifs requiert une assistance importante. Afin d'éviter aux chercheurs de trop dépendre de la disponibilité de l'administrateur, nous avons crée un nouvel utilisateur : groom.
Dès qu'il reçoit un mail il rend le service correspondant aux mots clé trouvés dans le Subject : forward de la messagerie (avec maintien éventuel d'une copie locale), annulation de ce forward, réinitialisation du mot de passe perdu, déblocage du process popper, etc.
Nos utilisateurs ayant bien adopté ce groom, face aux problèmes grandissants de sécurité, nous avons eu l'idée d'étendre ses fonctions à la gestion des accès extérieurs sur notre serveur de messagerie (station Unix).

■ Gestion automatique des accès extérieurs

Nous ne souhaitions pas que l'ouverture indispensable de notre serveur aux accès extérieurs entraîne, dans un contexte de laboratoires où les déplacements sont fréquents, des procédures contraignantes pour l'utilisateur ou lourdes pour l'administrateur. Après réflexion et consultation des utilisateurs, les principes suivants ont été retenus :

- par défaut une connexion, soit directe (*telnet*), soit via un client POP, est autorisée depuis tout laboratoire ou tout Institut du site,
- depuis l'extérieur, une seule adresse de connexion est autorisée par utilisateur à un moment donné,
- sur un compte donné, une connexion depuis le site est incompatible avec une connexion autorisée depuis l'extérieur,
- toute opération du groom déclenche deux *mail*s : un à l'expéditeur de la requête, l'autre au compte local. Ainsi un chercheur serait immédiatement alerté d'une demande de connexion extérieure utilisant son *login*.

Exemple

M. Dubois part aux US, à Berkeley. Devant la machine mise à sa disposition (MAC, PC ou station) il émet un *mail* vers groom@cnrs-grenoble.fr avec en *Subject* : telnet for dubois[1].

Le groom

- déduit du *mail* reçu de guest@berkeley.edu, l'adresse IP de la machine depuis laquelle Dubois souhaite travailler,
- dans la liste des machines autorisées à se connecter depuis l'extérieur, il ajoute cette adresse IP et l'associe au *login* dubois, ou remplace celle précédemment autorisée pour ce compte,
- envoie un *mail* à guest@berkeley.edu et à dubois@cnrs-grenoble.fr.

Si Dubois se déplace, il lui suffit de renvoyer le même *mail* pour aussitôt être autorisé à se connecter sur son compte depuis un nouveau poste.

Depuis le site :

- toute requête POP pour dubois (même authentifiée) sera rejetée tant qu'il y aura une autorisation de connexion distante associée à ce *login* (unPOP | untelnet dubois). Cependant les cas particuliers (un point fixe + un point mobile extérieurs) sont aisément supportés.
- à sa première connexion *telnet* locale, l'autorisation d'accès distant de Dubois est automatiquement supprimée. Cela lui est notifié à l'écran, et un *mail* est envoyé à guest@berkeley.edu ainsi qu'à dubois@cnrs-grenoble.fr.

Ainsi la contrainte pour le chercheur en déplacement est réduite à l'envoi d'un simple *mail*. Ses requêtes sont prises en compte immédiatement, 24h/24, 7j/7. De plus il est aidé :

[1] Syntaxe : telnet POP [for] *user* [from: *adresse*]

- avant d'accepter sa requête, le groom effectue les vérifications élémentaires pour que celle-ci soit cohérente,
- pour un accès POP, en se basant sur l'entête du *mail* reçu, le groom lui souffle le paramétrage complet pour son client POP (*EmailAddress*, *SMTP server*, etc.).

Pour le serveur le risque est réduit : ses ouvertures à l'extérieur collent aux déplacements du chercheur et sont limitées à son *login*.

L'administrateur de son côté est libéré de tâches répétitives et fastidieuses. La trace précise des connexions acceptées ou refusées, lui permet de repérer aisément une anomalie.

Pour mettre en œuvre ce mécanisme, le programme du groom s'appuie sur les logiciels suivants :

- tcp-wrapper : filtre les accès *ftp*, *rlogin*, etc., mais laisse passer *telnet.*
- logdaemon/login.c (source modifié) : accepte login et mot de passe, puis selon un fichier d'autorisation (mis à jour par le groom) accepte ou non la connexion.
- popper (source modifié) : s'appuyant lui aussi sur un fichier d'autorisation tenu à jour par le groom, il autorise ou non l'accès à la boite aux lettres du chercheur.

Le serveur ainsi automatisé peut servir de *fire-wall* : il suffit à un chercheur désirant protéger sa station de n'y autoriser que les connexions depuis le serveur.