Mettez du son dans votre pare-feu

Gazette Linux n°104 — Juillet 2004

Michael Hamilton

Article paru dans le n°104 de la Gazette Linux de juillet 2004.
Traduction française par Régis Perdreau `<regis POINT perdreau CHEZ tiscali POINT fr>`.
Relecture de la traduction française par Joëlle Cornavin `<jcornavi CHEZ club TIRET internet POINT fr>`.

Voici un petit script shell amusant pour les amateurs. Cet article décrit comment vous pouvez entendre littéralement les paquets émettre un son à chaque **ping** provenant de votre pare-feu.

Si votre systême Linux est doté d'un pare-feu géré par iptables, vous avez peut-être remarqué, dans le fichier `/var/log/messages` les lignes de journal signalant des paquets ignorés comme celle-ci :

J'ai pensé qu'il serait plus amusant d'avoir un retour audio de mon pare-feu. Pour cela, j'ai écrit un petit script qui émet un son chaque fois que qu'un paquet est refusé. Voici le script dans sa version la plus simple :

J'utilise **tail** avec l'option `follow=name` de façon à ce que le script continue à suivre le fichier des messages, même après une rotation des fichiers journaux effectuée par logrotate. Je redirige ensuite les messages dans **awk** et, si jamais **awk** voit une ligne entière ($0) contenant le texte DROP, je fais exécuter à awk une commande qui envoie un fichier `wav` codé sur 8 bits dans `/dev/audio`. Le résultat est un son ressemblement à un clic à chaque rejet d'un paquet par le pare-feu. En principe, je n'obtiens que quelques clics par heure. En cas d'attaque par un ver, ce taux peut s'accroître considérablement.

Ce script a fonctionné correctement, mais en fait je ne m'intéresse qu'aux ports qui pourraient exécuter des services. Pour les ports non associés à des services, je préfère que ce soit moins agressif. Pour ces quelques ports, j'ai pensé qu'il serait amusant de faire clignoter une des diodes du clavier. Une recherche sur www.freshmeat.org (http://www.freshmeat.org) m'a renvoyé à l'utilitaire tleds, qui fait clignoter les diodes selon l'activité du réseau. Après avoir étudié le source de telds, j'ai pu créer rapidement xblink, pour faire clignoter la diode d'arrêt de défilement chaque fois qu'elle reçoit un ligne d'entrée. Voici le code source de xblink :

Maintenant, je peux entendre un clic ou obtenir un clignotement. Il ne me reste plus qu'à améliorer mon script pour qu'il lise la liste des services connus dans `/etc/services`. Le voici :

La première partie du script awk, intitulée avec l'action **BEGIN**, est exécutée une fois lorsque le script démarre. Cette action lit une liste de services et les stocke dans une table de hachage de services indexée par numéro de port. La seconde partie met en correspondance toute ligne ($0) contenant DROP et extrait

l'adresse source et le port de destination du paquet. Pour chaque ligne correspondante, le script redirige une ligne à la commande **blink**. Pour les lignes correspondant à un service connu, il lance une commande **cat** qui envoie un fichier `wav` vers /dev/audio. Pour surveiller mon pare-feu, je me contente de lancer le script dans un xterm.

Les techiques employées ne se limitent pas à la surveillance par pare-feu. Vous pouvez lire des sons ou faire clignoter des diodes pour n'importe quelle sorte de surveillance.