pcapr.net, pour explorer des paquets réseau

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 janvier 2009. Dernière mise à jour le 31 juillet 2013

http://www.bortzmeyer.org/pcapr.html

Examiner en détail, au niveau des champs qui le composent et même des bits sous-jacents, des paquets capturés sur le réseau est une occupation essentielle pour l'étudiant en réseaux informatiques, pour le programmeur réseau, pour l'administrateur réseaux... et pour celui qui s'intéresse à la sécurité des réseaux. Des outils pour programmeur comme Scapy ou des outils graphiques très riches comme Wireshark permettent de rendre cette tâche bien plus efficace, pour les paquets qu'on a capturé soi-même. Mais il peut être instructif d'explorer les paquets capturés sur des réseaux différents du sien, par exemple pour apprendre des protocoles dont on n'a pas de mise en œuvre disponible. C'était l'un des buts de pcapr <http://www.pcapr.net>, le Flickr des paquets. Ce service semble malheureusement mort aujourd'hui.

Le principe est simple : vous vous enregistrez (gratuit mais obligatoire) et vous pouvez ensuite envoyer vos propres traces et/ou regarder celles envoyées par les autres membres. Du fait de l'inscription obligatoire, certains liens dans cet article ne seront pas accessibles tant que vous n'aurez pas un compte pcapr (actuellement, un visiteur anonyme peut avoir une idée des paquets mais pas les examiner en détail).

Vous pouvez chercher une trace (un ensemble de paquets) par date <http://www.pcapr.net/browse> ou par mot-clé (des étiquettes - "*tags*" -, comme dans del.icio.us). Si je m'intéresse à BGP et que le RFC 4271 [1] ne me suffit pas, je peux chercher <http://www.pcapr.net/browse?proto=bgp>. Si je préfère LDAP, j'ai <http://www.pcapr.net/browse?proto=ldap>.

Une fois la trace trouvée, je peux regarder les paquets, voir leur représentation binaire, ou bien voir une dissection des paquets (apparemment faite par tshark).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4271.txt

Cela permet déjà d'innombrables possibilités. On ne peut pas déployer tous les protocoles chez soi pour les essayer mais pcapr <http://www.pcapr.net/> permet d'accéder à des tas de protocoles différents. On peut aussi télécharger les traces chez soi au format Pcap pour les étudier plus à loisir, par exemple avec ses propres programmes en C <http://www.bortzmeyer.org/libpcap-c.html> ou en Python <http://www.bortzmeyer.org/libpcap-python.html>.

Mais pcapr a une autre possibilité : on peut modifier les paquets, via l'interface Web et copier ensuite la version modifiée (une sorte de Scapy sur le Web).

Terminons sur un avertissement : les traces Pcap peuvent contenir des informations confidentielles. Par exemple, les adresses IP permettent de retrouver une personne, celle qui utilisait cette adresse et sont donc considérées à juste titre par la CNIL comme des données personnelles <http://www.cnil.fr/index.php?id=2244>, relevant de la loi Informatique & Libertés. Pcapr étant situé aux États-Unis, qui n'ont pratiquement aucune protection légale de la vie privée, il faut donc n'envoyer que des traces :

— Anonymisées, par exemple par un programme d'anonymisation comme pktanon <http://www.tm.uka.de/software/pktanon/>, comme le plus riche et plus complexe Flaim <http://flaim.ncsa.illinois.edu/>, comme CoralReef <http://www.caida.org/tools/measurement/coralreef/>, ranonymize <http://www.qosient.com/argus/anonymization.htm>, Anontools <http://www.ics.forth.gr/dcs/Activities/Projects/anontool.html> ou encore IP : :Anonymous <http://search.cpan.org/~jtk/IP-Anonymous-0.04/lib/IP/Anonymous.pm>. Ces programmes remplacent chaque adresse IP par une valeur prise dans 192.0.2.0/24 ou 2001:DB8::/32, voire la suppriment totalement. Notez aussi l'option -h de dnscap <https://www.dns-oarc.net/tools/dnscap> si on l'a utilisé pour la capture. Attention, en utilisant les autres informations, il est parfois possible de retrouver quand même les identificateurs <http://www.schneier.com/blog/archives/2007/12/anonymity_and_t_2.html> qui avaient été anonymisés. C'est pour rendre cette « désanonymisation » plus difficile que la plupart des programmes cités ci-dessus mettent en œuvre des algorithmes complexes.
— Ou des traces ne montrant que des adresses IP « à vous », locales à votre réseau. (Ou encore, ce qui est fréquent lors des attaques, des adresses IP que l'on sait usurpées, et qui sont bien indiquées comme telles dans les commentaires de la trace. Voir par exemple <http://www.pcapr.net/view/bortzmeyer+pcapr/2009/0/4/13/dns-ns-dot-attack-january-2009.pcap.html>.)

Grâce à François Ropert, voici les adresses de services similaires :

— OpenPacket <https://www.openpacket.org/>
— EvilFingers <http://www.evilfingers.com/projects/pcaps.php> (sur ce dernier, il semble qu'on ne puisse pas envoyer ses propres traces, c'est moins Web 2.0...)

Sinon, l'idée de pcapr était séduisante mais, en pratique, le site semble avoir été abandonné en 2011-2012 (plus de nouveautés <http://www.pcapr.net/new>, dernier message automatique du site en août 2012). En juillet 2013, même le téléversement de nouveaux pcap ne marchait plus (« *"We are unable to process this pcap. Please see the faq for common upload problems."* » et aucun moyen de contacter un administrateur).