L’outil à tout faire des connexions réseau.

Son auteur le définit comme un couteau suisse. Il s’agit de Netcat (Network cat). Un petit programme versatile à souhait qui va se nicher, pardon, se connecter n’importe où.
Yannick Cadin

Singer Mail

$ echo -e 'MAIL FROM:yannick@diablotin.info\nRCPT TO:carole@onsefaitla.biz\nDATA\nCourrier avec Netcat\n.\nQUIT' | nc mail.wanadoo.fr smtp

nc (Netcat en abrégé) reçoit sur son entrée standard tout le texte émis avec la commande echo (son option -e permet l’emploi de séquences comme \n pour représenter les retours chariot). Les lignes ainsi reçues sont envoyées telles quelles à l’ordinateur de nom mail.wanadoo.fr sur son port de communication numéro 25 (nc trouve la correspondance smtp <=> 25 en allant regarder dans le fichier /etc/services).
La caractéristique principale de nc est de ne faire absolument aucune interprétation (aucune manipulation) sur les données qu’il envoie où qu’il réceptionne. Il se distingue ainsi de l’outil plus spécialisé qu’est telnet.

Singer un serveur Web

$ nc -l -p 8000

Après avoir lancé la commande ci-dessus, allez dans Firefox et saisissez http://localhost:8000/ comme URL à consulter puis retournez dans votre fenêtre Terminal pour voir ce qui est apparu.
nc se révèle être un allié très utile dès qu’il s’agit d’appréhender les messages échangés dans une communication entre un client et un serveur pour un protocole donné. Ici on découvre très exactement ce que notre navigateur soumet à un serveur Web pour en obtenir la page d’accueil.
L’option -l signifie "Listen" ("écouter" par opposition à émettre qui est le comportement par défaut de nc). L’option -p précise sur quel port de communication il faut attendre la connexion. Le choix ici de la valeur 8000 est totalement arbitraire. La seule contrainte est de prendre un nombre supérieur à 1023 car les ports de 1 à 1023 ne peuvent être « écoutés » que par root.

Scruter les ports

$ nc -w 3 -z -v MACHINE_CIBLE 1-600

Les prémisses du piratage ! Voici ce que l’on appelle un « scan de port ». Rudimentaire certes mais suffisant pour découvrir quels sont les ports de communication à l’écoute (recherche limitée à l’intervalle 1 à 600 dans l’exemple présent) sur l’ordinateur de nom MACHINE_CIBLE.
Au-delà d’intentions malveillantes, cette utilisation de nc peut servir à vérifier le bon fonctionnement d’une machine en s’assurant que les services qu’elle est censée offrir sont toujours disponibles (simplement parce que les ports réseau correspondants restent « ouverts », autrement dit à l’écoute).
À noter qu’il est possible de faire la même chose pour trouver les ports sur lesquels la communication s’établit en UDP en ajoutant juste l’option -u dans la commande ci-dessus (mais le traitement peut s’avérer beaucoup plus long).

Sauvegarde en réseau

POSTE_DST$ nc -l -p 4000 | tar xz

La présente commande est à lancer sur la machine qui doit accueillir les fichiers à copier, depuis le dossier qui les recevra. La commande qui suit,

POSTE_SRC$ tar cz . | nc -w 3 ADRESSE_IP_POSTE_DST 4000

Est à exécuter depuis le dossier à dupliquer sur l'ordinateur source. Il est dit sur la première que tout ce qui arrivera sur le port 4000 devra être soumis à la commande tar (qui va désarchiver comme le mentionne son option x des données compressées, ce que précise son option z). Sur la machine source, on construit l'archive compressée (options c et z) avec les fichiers du dossier courant (symbolisé par un point) que l'on confie à nc pour un envoi sur la première machine. L'option -w indique qu'après 3 secondes d'inactivité, il conviendra de clore la connexion.

Aspirateur de pages Web

$ echo -e 'GET /prestations/\n' | nc diablotin.com http > page.htm

Une version ultra simplifiée de ce que fait en temps normal un navigateur Web. Certainement le moyen le plus rapide de télécharger un document HTML. Je vous laisse imaginer les perspectives. Il devient par exemple trivial de détecter les modifications de contenu sur des sites que vous visitez régulièrement, simplement en appliquant la commande cmp (ou diff) sur des documents ainsi rapatriés à différentes époques.

Convertir en ligne des euro en dollars au taux de change en cours

$ echo -e 'POST /ucc/convert.cgi HTTP/1.0\nContent-Length:
25\n\nAmount=50&From=EUR&To=USD' | nc www.xe.com http | sed -n 's/^.*<B>\([0-9.]*\)
USD<.*$/\1/p'

Plus complexe, on interroge cette fois un serveur Web qui propose de faire des conversions de devises. On fabrique la requête que l'on soumet à nc à l'aide de la commande echo et l'on extrait de la réponse (une longue page en HTML) l'unique donnée qui nous intéresse. Comment ? Grâce au programme sed que nous avons étudié le mois dernier. Vous voyez bien que ça sert :-)