La commande TCPDUMP

Tcpdump a été initialement développé en 1988 par Van Jacobson, Sally Floyd, Vern Paxson et Steven McCanne. Ils travaillaient au Lawrence Berkeley Laboratory Network Research Group.

Il permet à ses utilisateurs d'afficher les paquets TCP/IP et autres qui sont reçus et transmis sur le réseau. Il fonctionne sur la plupart des systèmes d'exploitation basés sur Linux. Il utilise la bibliothèque libpcap pour capturer les paquets, qui est une bibliothèque basée sur C/C++. Tcpdump a également un équivalent Windows. Il s'appelle windump. Il utilise la bibliothèque winpcap.

20:58:26.765637 IP 10.0.0.50.80 > 10.0.0.1.53181: Flags [F.], seq 1, ack 2, win 453, options [nop,nop,TS val 3822939 ecr 249100129], length 0

Chaque ligne comprend

* Horodatage Unix (20:58:26.765637)
* protocole (IP)
* le nom d'hôte ou l'adresse IP source et le numéro de port (10.0.0.50.80)
* nom d'hôte ou IP de destination et numéro de port (10.0.0.1.53181)
* Indicateurs TCP (Flags [F.]). Les drapeaux indiquent l'état de la connexion. Cela peut inclure plus d'une valeur, comme dans cet exemple [F.] pour FIN-ACK. Ce champ peut avoir les valeurs suivantes:
  + S - SYN. La première étape de l'établissement de la connexion.
  + F - FIN. Terminaison de la connexion.
  + . - ACK. Paquet d'accusé de réception reçu avec succès.
  + P - POUSSER. Indique au récepteur de traiter les paquets au lieu de les mettre en mémoire tampon.
  + R - RST. La communication s'est arrêtée.
* Numéro de séquence des données dans le paquet. (seq 1)
* Numéro d'acquittement (ack 2)
* La taille de la fenêtre (win 453). Le nombre d'octets disponibles dans le tampon de réception. Ceci est suivi des options TCP.
* Longueur de la charge utile de données. (length 0)