Analyseurs réseau (sniffers)

Juin 2014

L'analyse de réseau

Un « **analyseur réseau** » (appelé également *analyseur de trames* ou en anglais *sniffer*, traduisez « renifleur ») est un dispositif permettant d'« écouter » le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent.

En effet, dans un réseau non commuté, les données sont envoyées à toutes les machines du réseau. Toutefois, dans une utilisation normale les machines ignorent les paquets qui ne leur sont pas destinés. Ainsi, en utilisant l'interface réseau dans un mode spécifique (appelé généralement *mode promiscuous*) il est possible d'écouter tout le trafic passant par un adaptateur réseau (une carte réseau ethernet, une carte réseau sans fil, etc.).

Utilisation du sniffer

Un sniffer est un formidable outil permettant d'étudier le trafic d'un réseau. Il sert généralement aux administrateurs pour diagnostiquer les problèmes sur leur réseau ainsi que pour connaître le trafic qui y circule. Ainsi les détecteurs d'intrusion (*IDS*, pour *intrusion detection system*) sont basés sur un sniffeur pour la capture des trames, et utilisent une base de données de règles (*rules*) pour détecter des trames suspectes.

Malheureusement, comme tous les outils d'administration, le sniffer peut également servir à une personne malveillante ayant un accès physique au réseau pour collecter des informations. Ce risque est encore plus important sur les réseaux sans fils car il est difficile de confiner les ondes hertziennes dans un périmètre délimité, si bien que des personnes malveillantes peuvent écouter le trafic en étant simplement dans le voisinage.

La grande majorité des protocoles Internet font transiter les informations en clair, c'est-à-dire de manière non chiffrée. Ainsi, lorsqu'un utilisateur du réseau consulte sa messagerie via le protocole POP ou IMAP, ou bien surfe sur internet sur des sites dont l'adresse ne commence pas par HTTPS, toutes les informations envoyées ou reçues peuvent être interceptées. C'est comme cela que des sniffers spécifiques ont été mis au point par des pirates afin de récupérer les mots de passe circulant dans le flux réseau.

Les parades

Il existe plusieurs façons de se prémunir des désagréments que pourrait provoquer l'utilisation d'un sniffer sur votre réseau :

- Utiliser des protocoles chiffrés pour toutes les communications dont le contenu possède un niveau de confidentialité élevé.

- Segmenter le réseau afin de limiter la diffusion des informations. Il est notamment recommandé de préférer l'utilisation de switchs (*commutateurs*) à celle des hubs (*concentrateurs*) car ils commutent les communications, c'est-à-dire que les informations sont délivrées uniquement aux machines destinataires.
- Utiliser un détecteur de sniffer. Il s'agit d'un outil sondant le réseau à la recherche de matériels utilisant le mode *promiscuous*.
- Pour les réseaux sans fils il est conseillé de réduire la puissance des matériels de telle façon à ne couvrir que la surface nécessaire. Cela n'empêche pas les éventuels pirates d'écouter le réseau mais réduit le périmètre géographique dans lequel ils ont la possibilité de le faire.

Plus d'informations

- Ethereal, le célèbre analyseur de protocoles
- TCP dump
- WinDump, portage de TCP dump sous Windows

Network analyzers (sniffers) Analizadores de red (rastreadores de puertos) Netzwerk-Analysator (sniffer) Analizzatori di rete (sniffer) analisadores redes (sniffers)