Analyse du trafic réseau

Par Patrick Sentinel – 29a.ca

📡🔬 Analyse du trafic réseau : quand lire des paquets devient un art martial

Imagine que ton réseau est une autoroute. Il y a des voitures (les paquets), des sorties (les ports), des fous du volant (les hackers), et… toi, au bord de la route, avec une paire de jumelles et *Wireshark* dans les mains. Bienvenue dans le monde intense et fascinant de l'analyse de trafic réseau, aussi appelée : *"J'ai ouvert un paquet et je suis tombé sur un mot de passe en clair."*

🕵️‍♂️ Pourquoi inspecter les paquets?

Parce qu'ils parlent… Beaucoup. Ils révèlent ce qui entre et sort de ton réseau. Ils montrent qui parle à quoi, comment, et pourquoi à 3h du matin. Et parfois, ils disent des choses qu'ils ne devraient pas. (Exemple: ton mot de passe FTP envoyé en clair depuis 2006.) L'analyse de trafic, c'est comme lire les textos de ton réseau. Sauf que c'est **légal**. Et, tu découvres que ton grille-pain parle portugais et allemand.

🧠 Outils du ninja réseau

🐬 Wireshark

L'outil roi. Il capture tout, tout le temps. Tu veux voir ce que fait *Google Chrome* à chaque milliseconde? T'inquiète, il t'enverra 45 000 paquets par minute, juste pour dire "bonjour".

📝 tcpdump

Plus rustique, plus sobre, mais plus rapide. C'est *Wireshark* sans le maquillage. Il t'envoie la vérité, ligne après ligne, sans pitié, sans émoticons.

🛠️ Zeek, Suricata ou autre bébelle du genre

Quand tu veux de l'analyse automatisée, des logs clairs, et moins de sueur frontale.

Que trouve-t-on dans un paquet?

- IP source et destination (qui parle à qui);
- Port source et destination (pour faire quoi);
- Protocole (TCP? UDP? ICMP? Le nouveau protocole obscur de l'imprimante démoniaque?);
- *Payload* (le contenu. Genre… ton mot de passe, si tu vis dangereusement.).

Les surprises du métier :

Voir que ton téléviseur essaie de contacter 7 serveurs en Chine à chaque mise sous tension. Découvrir que ton voisin t'envoie des requêtes ARP tous les matins à 6h42. Observer un scan de ports… alors que *toi-même* tu croyais ne rien faire.

Comment survivre à un dump de 50 000 paquets :

Filtre tout de suite.
Pas de filtre = noyade cérébrale. Utilise des filtres simples dans *Wireshark* :

ip.addr == 192.168.1.42

tcp.port == 443

http.request.method == "POST"

Cherche les anomalies.

Trop de paquets trop vite?

Requêtes bizarres?

Un frigo qui envoie un fichier ZIP?

Respire. Prends un thé ou café… Ce n'est pas parce que tu vois un "SYN" que tu es attaqué. C'est peut-être juste *Netflix* qui fait des câlins à ton routeur.

En résumé :

L'analyse du trafic réseau, c'est un peu comme écouter les conversations d'un party où tout le monde parle en binaire. Tu ne comprends pas toujours tout, mais quand tu comprends… *tu ne peux plus faire semblant d'avoir rien vu*. Alors attrape ton *Wireshark*, ouvre les yeux, et rappelle-toi : Ce n'est pas toi qui lis les paquets. Ce sont eux qui te révèlent les secrets de ton réseau.
