pktmon : analyser et capturer des paquets réseaux de Windows 10

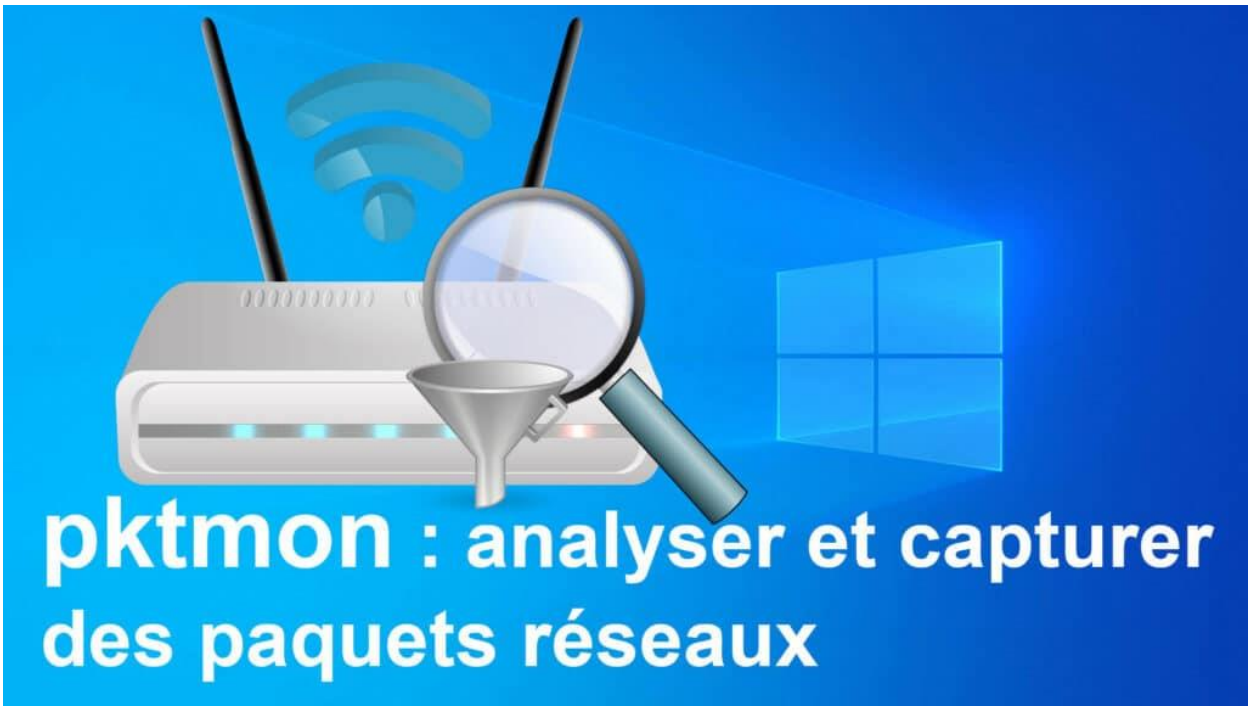
Pour capturer des paquets réseaux, on connait Wiresharck. Mais Windows 10 possède aussi un outil internet : **pktmon**

Il fonctionne un peu de la même manière que tcpdump sur Linux. Rappelons aussi que Windows 10 possède l'outil **netsh trace** pour capturer les paquets.

Microsoft a ajouté pktmon pour sniffer les paquets réseau dans la mise à jour d'octobre 2018 de Windows 10.

Les captures de paquets se font au format ETL mais on peut les convertir en PCAPNG. De quoi les lire dans tcpdump ou Wiresharck.

Voici un aperçu de l'outil **pktmon** pour analyser vos connexions réseaux en profondeur.



Le programme se trouve dans C:\Windows\system32\pktmon.exe. Il fonctionne en invite de commandes en administrateur. L'aide nous donne comme description de l'outil : *Surveiller les rapports internes de propagation de paquets et de rejet de paquet*.

a) Les commandes suivantes sont disponibles :

- **filtre** : pour gérer les filtres de paquets
- **comp** : gérer les composants enregistrés
- **réinitialiser** : réinitialiser les compteurs à zéro
- **démarrage** : démarrer la surveillance des paquets
- **stop** : stopper la surveillance des paquets
- **format** : convertir le fichier journal en texte
- **décharger** : décharger le pilote PktMon

b) Capturer les paquets sur un port

La capture se fait en deux parties comme avec wiresharck.

- On configure les filtres, comme les ports réseau à écouter
- puis on démarre la capture que l'on peut ensuite arrêter

c) Configurer les filtres

On utilise la commande **filter** en indiquant le port de cette manière : **pktmon filter add -p 53**

Rien empêche de paramétrer plusieurs filtres afin d'écouter sur différents ports par exemple. Mais on peut aussi filtrer sur le protocole avec le paramètre –t : **pktmon filter add -t TCP**

Comme vous pouvez le voir, pas mal d'option dont -d pour jouer sur l'IPv4 et l'IPv6.

- Pour lister les captures, on utilise le paramètre **list** : **pktmon filter list**
- Enfin pour supprimer TOUS les filtres : **pktmon filter remove**

d) Démarrer la capture des paquets réseaux

Vous savez maintenant comment paramétrer les filtres afin d'écouter les ports souhaités. Il ne reste plus qu'à démarrer la capture de paquets.

On utilise alors la commande **start**. Une fois exécuté, pktmon enregistrera tous les paquets sur TOUTES les interfaces réseau de l'appareil dans un fichier appelé **PktMon.etl** et n'enregistrera que les 128 premiers octets d'un paquet : **pktmon start --etw**

Voici la commande à utiliser pour afficher les paquets capturés directement dans l'invite de commandes. Cela ne fonctionne qu'à partir de Windows 10 2004 : **pktmon start --etw -m real-time**

Enfin si vous désirez filtrer les captures sur une interface réseau en particulier, cela est aussi possible. On utilise alors la commande de cette manière : **pktmon start --etw -p 0 -c XX**
XX est l'ID de l'interface réseau à capturer.

Vous pouvez obtenir les ID avec la commande suivante : **pktmon comp list**

Enfin pour arrêter, la capture on utilise **stop** : **pktmon stop**

e) Convertir les formats de fichiers journaux de capture réseau

Par défaut, le fichier journal de capture de paquets est **PktMon.etl**.
Mais on peut convertir ce dernier en texte ou au format pcap.

Le programme Microsoft Network Monitor permet de lire le fichier **etl**. Ainsi vous pouvez étudier la capture réseaux, appliquer des filtres faire des recherches, etc. Enfin le programme peut aussi enregistrer et convertir le fichier etl en fichier .cap.

Mais PktMon permet aussi de convertir le fichier etl en fichier Texte. Pour cela, on utilise l'option **format** qui permet de convertir les fichiers journaux de capture réseau. Par exemple pour le convertir en texte : **pktmon format PktMon.etl -o dns.txt**

f) Liens et autres outils capture réseaux

Il existe un article sur le site concernant l'outils WireSharck pour sniffer, capturer et faire des analyses réseaux ➔ WireShark : sniff et analyse réseau

Process Monitor (ProcMon) peut aussi faire le job selon ce que vous souhaitez enregistrer au niveau de l'activité réseau.

Enfin une liste de logiciels pour suivre l'activité système de Windows dont le réseau : Les meilleurs logiciels pour suivre l'activité système Windows

Et des liens réseaux Windows 10 :

- Windows 10 : mesurer l'utilisation réseau
- Lister les connexions réseau sur Windows