|  |  |  |
| --- | --- | --- |
|  | **tcpDump** | |
| **DESC** | | Capture et analyse réseaux basé sur libpcap |
| **CONF** | |  |
| **OPTS** | | |
| -S | | Suit les connexions TCP (Consomme RAM) |
| -p | | Bloque le mode promiscous : n’écoute que le trafic à destination de la machine |
| -n|nn | | -n pas de conversion n°IP[& n°Port] -> Noms (Evite les recherches DNS) et donc évite de ralentir la machine |
| -i <interface> | | Par défaut la première interface, si any : écoute toutes les interfaces |
| -D | | List des interfaces dispos pour la capture |
| -w <file.pcap> | | Enregistrement de l’écoute |
| -C 10 | | Si fichier rempli à plus de 10 mb, création d’un deuxième fichier |
| -W 5 | | Rotation sur 5 fichiers d’écritures. A utilisé avec -C |
| -r <file> | | Affiche le fichier .pcap ou .tcpdump dans un format readable  A combiner avec wc –l pour #paquets du fichier |
| -s 0 | | Taille maxi d’un paquet capturé. 0=Intégralité du paquet peu importe la taille |
| -v | | 3 niveaux |
| -X | | Affiche les paquets en hexa et ASCII |
| -A | | Affichage contenu des paquets |
| -t | | Human readable timestamp |
| -e | | + ethernet header |
| -E <key> | | Decrypt IPSec |
| -c 10 | | Capturer 10 paquets uniquement |
| <Filtres> | | Pour ne filtrer qu’une partie du trafic |
| **Comments :**  BPF -> filtre  ( doit être échappé pour éviter interprétation du BASH ou mettre ‘…’ sur l’ensemble  host hostname  port #port|Protocole  portrange X-Y  And, or, (), and not, &, |, !… : combinaison de règles  IP… : filtrage par protocole  src, dst  Less X, greater Y, <= Z : particular size  tcp[X] : pour les flags  Si paquets dropped : augmenter taille des buffers réseaux (sockets) | | |