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