|  |  |  |  |
| --- | --- | --- | --- |
| **Suricata** | | | |
| **DESC** | IDS/IPS | | |
| **CLI** | | | |
| **GENERALE** | | | |
| -h | brief usage | | |
| -V | version | | |
| -T | Test configuration | | |
| -v | verbosity | | |
| -T | Test configuration | | |
| --set <key>=<value> | Overiding d’un paramètre du fichier de conf | | |
| --engine-analysis | Analyse du moteur | | |
| **INFORMATIONS** | | | |
| --dump-config | Affichage du fichier de configuration sur le terminal | | |
| --build-info | Comment Suricata a été installé | | |
| --list-app-layer-protos | Tous les protocoles applicatifs supportés | | |
| **RUNNING** | | | |
| **OBLIGATOIRE** | | | |
| -r <path> | Read PCAP file. Offline mode | | |
|  | --pcap-file-delete | Suppression des pcap une fois traités | |
| -i <interface> | Analyse temps réel  Choisis la meilleure méthode de capture | | |
| **CONFIGURATION LANCEMENT** | | | |
| -c <path> | Path to conf file | | |
| -s <file.rules> | Ce fichier + les règles dans fichier yaml seront utilisés. | | |
| -S <file.rules> | Utiliser uniquement ce fichier comme set de règles. | | |
| -l <directory> | Répertoire de logs. Sinon défaut | | |
| -D | Lance le processus en arrière-plan | | |
| Filtres | Not host 1.1.1.1 | | Les paquets en dehors ne seront pas traités par Suricata |
| Tcp or udp | |
| Not (host X or IP2 or NET/24) | |
| **MODE** | | | |
| --pcap[=<device>] | PCAP mode | | |
| --af-packet[=<device>] |  | | |
| --netmap[=<device>] |  | | |
| --pfring[=<device>] |  | | |
| --pfring-cluster-id <id> |  | | |
| --pfring-cluster-type <type> |  | | |
| -q <queue id> | NFQUEUE | | |
| --runmode <runmode> | Workers|autofp|single | | |
| **OPTIMISATION** | | | |
| --pcap-buffer-size=<size> | 0 – 2147483647 | | |
| **Comments :** | | | |