|  |  |  |
| --- | --- | --- |
| **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 | |
| **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 :** | | |

|  |  |
| --- | --- |
| **TRASH** | |
| --pcap-file-continuous | -r |
| --pcap[=<device>] |  |
| --af-packet[=<device>] |  |
| -q <queue id> |  |
| --runmode <runmode> | Workers, autofp, single |
| -F <bpf filter file> |  |
| -k [all|none] | Check du checksum ou non |
| --user=<user> |  |
| --group=<group> |  |
| --pidfile <file> | Ecris le pid du process |
| --init-errors-fatal | Si erreur de lecture signatures, exit |
| --disable-detection | Désactive le detection engine |
| --dump-config | Ecrit le fichier de conf dans le terminal et exit |
| --build-info |  |
| --list-app-layer-protos | Ts les protocoles de couche supportés |
| --list-keywords = [all|csv|<kword>] | Mots-clefs de règles |
| --list-runmodes |  |
| --set <key>=<value> |  |
| --engine-analysis |  |
| --unix-socket=<file> |  |
| --pcap-buffer-size = <size> | De 0 à 2147483647 |
| --netmap[=<device>] |  |
| --pfring[=<device>] |  |
| --pfring-cluster-type <type> |  |
| -d <divert-port> | Run inline |
| --dag <device> |  |
| --napatech |  |
| --mpipe |  |
| --erf-in=<file> | Offline mode via ERF file |
| --simulate-ips | When IDS. |
| **Comments :** | |