|  |  |  |  |
| --- | --- | --- | --- |
|  | **Suricata** | | |
| **DESC** | | IDS/IPS | |
| **FILES AND DIRECTORY** | | | |
| /etc/ suricata/ suricata.yaml  Rules/ | | Conf  Rules | |
| /var/log/suricata/ suricata.log  Stats.log  Fast.log  Eve.json  http.log | | Logs du lancement de Suricata  Stats post Suricata  Logs des alertes  ?  ? | |
| /var/run/suricata.pid | | PID du démon si renseigné dans conf | |
| **SIGNAUX** | | | |
| SIGUSR2 | | | Live rule reload |
| SIGHUP | | | Close and reopen log file |
| **OPTS** | | | |
| **INFORMATIONS** | | | |
| -h | | | brief usage |
| -v | | | version |
| -c <path> | | | Path to conf file |
| -T | | | Test configuration |
| -v | | | verbosity |
| -r <path> | | | Read PCAP file. Offline mode |
| --pcap-file-continuous | | | -r |
| -i <interface> | | | Real time analysis  Choisis la meilleure méthode de capture |
| --pcap[=<device>] | | |  |
| --af-packet[=<device>] | | |  |
| -q <queue id> | | |  |
| -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 |
| --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. | |
| **DEV** | | | |
| -u | | Run unit tests and exit | |
| -U, --unittest-filter=REGEX | |  | |
| --list-unittests | | List all unit tests | |
| --fatal-unittests | | Un fail lors d’un Unit test : on exit au lieu d’enchainer sur les autres tests | |
| --unittests-coverage | | Display les résultats de tests unitaires | |
| **CONF** | | | |
| Max-pending-packets | | Nombre de paquets processed simultanément.  Compromis perf/RAM | |
| runmode | | Autofp… | |
| Default-packet-size | | Mettre la taille des paquets la plus couramment utilisée (ex 1514) | |
| Run-as : | | Users+group | |
| Pid-file : <file> | | Record le PID du daemon. | |
| mpm-algo: <ac|hs|ac-bs|ac-ks> | | Pattern matcher algo | |
|  | |  | |
|  | |  | |
|  | |  | |
|  | |  | |