**Suricata**

|  |  |  |  |
| --- | --- | --- | --- |
| **DESC** | | | |
| IDS/IPS | | | |
| **FILES** | | | |
| /etc/suricata/ | Suricata.yaml | Configuration | |
|  | Rules/ | Règles | |
|  | Classification.config | Classement des niveaux d’alertes en fonction du classtype de la règle  Se retrouve dans alert\_category au niveau de l’alerte | |
|  | Reference.config | Permet de définir des alias à utiliser avec l’option référence de la règle | |
| /var/ | Log/suricata/ | Suricata.log | Logs internes à Suricata |
|  |  | Stats.log | Statistiques post Suricata |
|  |  | Fast.log | Logs des alertes rapides |
|  |  | Eve.json | Logs des alertes en JSON |
|  |  | http.log |  |
|  | /run/suricata.pid | PID du démon si renseigné dans la configuration | |
| **QUICK START** | | | |
| * Suricata -i <interface> | | | |

**Généralités :**

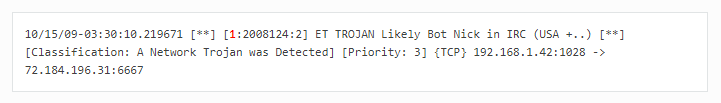
**Signaux :**

|  |  |
| --- | --- |
| **Signal** | **Comments** |
| SIGUSR2 | Live rule reload |
| SIGHUP | Close and reopen log file |

**Fichier de configuration :**

|  |  |
| --- | --- |
| **Directive** | **Comments** |
| **OBLIGATOIRE** | |
|  |  |
| **OPTIMISATION** | |
|  |  |
| **SECURITE** | |
|  |  |

**Format d’une alerte :**



[**GID** :SID :REV]

|  |  |
| --- | --- |
| **TRASH** | |
| 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 |