|  |  |  |
| --- | --- | --- |
|  | **Template** | |
| **DESC** | |  |
| **CONF** | |  |
| **OPTS** | | |
|  | |  |
|  | |  |
|  | |  |
| **Comments :** | | |

|  |  |  |
| --- | --- | --- |
|  | **Logwatch** | |
| **Desc** | | Surveille les journaux systèmes et crée des rapports. |
| **Conf** | | /usr/share/logwatch/default.conf/logwatch.conf (@dest des rapports, niveau de prio…) |
| **Opts** | |  |

|  |  |  |
| --- | --- | --- |
|  | **rsyslog** | |
| **Desc** | |  |
| **Conf** | | /etc/rsyslog.conf |
| **Opts** | |  |

|  |  |  |
| --- | --- | --- |
|  | **logrotate** | |
| **Desc** | | Permet de limiter la tailles des journaux systèmes |
| **Conf** | | /etc/logrotate.conf |
| **Opts** | |  |

|  |  |  |
| --- | --- | --- |
|  | **Cron** | |
| **DESC** | | Gestionnaire de tâches régulières |
| **CONF** | | /etc/ |
| **OPTS** | |  |

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

|  |  |  |
| --- | --- | --- |
|  | **tcpReplay** | |
| **DESC** | | Editing and replay trafic |
| **CONF** | |  |
| **OPTS** | | |
| **-i <interface> <file.pcap>** | |  |
| **-t** | | AQAP |
| **-M 10** | | Replay @ 10Mbps |
| **--stats=X** | | Stats every X seconds |
| **-p 25** | | Replay at 25 pps |
| **-o** | | For debuging |
| **--verbose** | |  |
| **-l X** | | Replay file X times (X=0 -> forever) |
| **-q** | | Quiet mode : no output |
| **Comments :**  Livré avec tcpRewrite : pour changer les IPs etc… afin d’anonymiser le fichier .pcap | | |

|  |  |  |
| --- | --- | --- |
|  | **iperf** | |
| **DESC** | |  |
| **CONF** | |  |
| **OPTS** | | |
|  | |  |
|  | |  |
|  | |  |
| **Comments :** | | |

|  |  |  |
| --- | --- | --- |
|  | **ntopng** | |
| **DESC** | | Monitoring réseau |
| **CONF** | |  |
| **OPTS** | | |
| **-i <interface>** | |  |
|  | |  |
|  | |  |
| **Comments :** | | |

|  |  |  |
| --- | --- | --- |
|  | **nagios** | |
| **DESC** | | Monitoring réseau |
| **CONF** | |  |
| **OPTS** | | |
|  | |  |
|  | |  |
|  | |  |
| **Comments :** | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **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** | | | |
| -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 | |
|  | |  | |
|  | |  | |
|  | |  | |
|  | |  | |