**Oinkmaster**

|  |  |
| --- | --- |
| **DESC** | |
| Update automatique des règles Snort  Programme ancestral | |
| **FILES** | |
| - | - |
| **QUICK START** | |
| * Renseigner url dans oinkmaster.conf et mettre ce fichier dans /etc/ * ./oinkmaster.pl –o <rules\_dest> | |

**Généralités :**

* Emerging threat (ET) :

<https://rules.emergingthreats.net/open/suricata-4.0/>

* Possibilité d’aller chercher les nouvelles règles sur le net, sur un fichier local ou distant (scp..)
* Oinkmaster va mettre exactement les nouvelles règles dans le répertoire, ni plus ni moins. On peut donc définir un skip files dans la configuration pour éviter qu’Oinkmaster ne supprime nos règles locales à chaque MAJ.

A vérifier peut être qu’il laisse justement les fichiers où il n’y a aucune MAJ à faire (exemple local.rules)

* Ne pas activer/désactiver des règles avec #, Oinkmaster remettra par défaut à son prochain lancement. Utiliser plutôt les SID.

**Oinkmaster.conf :**

|  |  |  |
| --- | --- | --- |
| **Paramètre** | **Comments** | |
| **GENERALE** | | |
| url | Lien de téléchargement des règles | |
| path | Path à utiliser pour les commandes bash que va utiliser Oinkmaster | |
| tmpdir | Par défaut /tmp/ (donc on peut laisser commenter)  Ce répertoire doit exister lors du lancement. | |
| umask | Si on veut overrider l’umask du système | |
| update\_files | Les fichiers qui doivent être mis à jour  Utilisation des REGEX | |
| include <file> | Inclusion d’un fichier de configuration.  Override des paramètres en fonction de la place de l’include | |
| skipfile local.rules | Evite qu’Oinkmaster ne supprime nos règles du fichier local.rules | |
| **RELATIVE AUX REGLES** | | |
| Modifysid | <SID> [, SID2…] "replace this" | "with this"  Utilisation des REGEX | |
|  | <file> "replace this" | "with this"  Utilisation du \* possible dans <file> | |
| enablesid <SID> | Dé-commente une règle commentée | |
| disablesid <SID> [, <SID2>…] | |  |