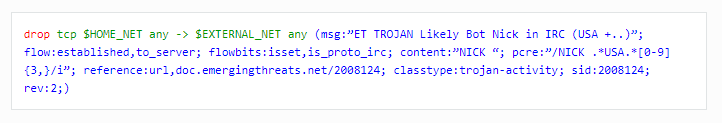
**Rules**

**Généralités :**



**Action** **Header** **Options**

**Actions :**

|  |  |
| --- | --- |
| **Action** | **Comment** |
|  |  |

**Header :**

Source -> destination

|  |
| --- |
| **Protocole** |
| Tcp | udp | icmp | ip |
| http | ftp | tls | smb | dns | ssh | smtp | imap | msn | ntp | dhcp… |

|  |  |
| --- | --- |
| **IP** | **Comment** |
| !1.1.1.1 | Tout sauf 1.1.1.1 |
| ![1.1.1.1,2.2.2.2] | Tout sauf 1.1.1.1 et 2.2.2.2 |
| $HOME\_NET |  |
| [10.0.0.0/24, !10.0.0.5] | Ce sous réseau sauf 10.0.0.5 |
| any |  |

|  |  |
| --- | --- |
| **Port** | **Comment** |
| [80,81,82] | Ces 3 ports |
| [80 :82] | Du 80 au 82 |
| [80 :] | Du 80 jusqu’au max |
| !80 | Tout sauf 80 |
| [1 :80, ![2,4]] | Du 1 au 80 sauf 2 et 4 |

|  |  |
| --- | --- |
| **Direction** | **Comment** |
| -> | unidirectionnel |
| <> | Bidirectionnel |

**Options :**

(<keyword> :<settings> ; <keyword> ;…)

; et " et \ doivent être échappés.

**Options :**

|  |  |
| --- | --- |
| **Génériques** | **Comment** |
| msg: "message" ; | Premier keyword de la signature  Se retrouve dans alert\_signature dans l’alerte |
| sid : 123 ; | Chaque signature possède son propre SID  Dernier keyword de la signature |
| rev :123 ; | Version de la signature  Vient après sid |
| gid :123 ; | Group ID  Pas vraiment utilisé, on laisse la valeur par défaut à 1 |
| classtype :trojan-activity ; | Avant dernière option  Se retrouve dans alert\_category dans l’alerte  Le fichier classification.config définit une priorité pour chaque classtype |
| reference : url, www.info.com | Infos sur la règle  Ici, url est remplacée par le champ url de reference.config :  url = http:// |
| priority :1 ; | De 1 à 255  Override du classtype et sa priorité associée dans classification.config |
| metadata : key value, key value ; | Métadonnée à ajouter dans l’alerte |
| target :[src\_ip|dest\_ip] | Spécifie qui est la cible de l’attaque |

|  |  |  |
| --- | --- | --- |
| **IP** | **Comment** | |
| ttl :10 ; |  | |
| ipopts : <name> ; | Check existence d’une option IP | |
|  | rr | Record route |
|  | eol | End of list |
|  | nop | No op |
|  | ts | timestamp |
|  | sec | IP security |
|  | esec | Extended IP security |
|  | lsrr | Loose source routing |
|  | ssrr | Strict source routing |
|  | satid | Stream identifier |
|  | any | Toutes les options sont mises |
| sameip ; | Même source et déstination | |
| ip\_proto :ICMP ; | ICMP|TCP|UDP|GRE|ESP|AH|IPv6-ICMP|… | |
| id :<number> ; | Fragment ID du paquet  Rappel : 1 fragment ID regroupe plusieurs fragments, classé par l’offset | |
| geoip : src, RU ;  geoip : both, CN, RU ;  … | Both|any|dest|src  Check du lieu géographique | |
| fragbits :<> | M|D|R  More, dont fragmant, reserved | |
| Fragoffset :[ !|<|>] <number> ; |  | |

|  |  |
| --- | --- |
| **ICMP** | **Comment** |
| itype :min<>max ;  itype :[<|>]<number> ; |  |
| icode :min<>max ;  icode :[<|>]<number> ; |  |
| icmp\_id :<number> ; |  |
| icmp\_seq :<number> ; |  |

|  |  |
| --- | --- |
| **TCP** | **Comment** |
| seq :0 ; | Numéro de séquence |
| ack :1 ; |  |
| Window :[ !]<number> ; | Fenêtre de réception |

|  |  |  |
| --- | --- | --- |
| **Payload** | **Comment** | |
| content :"….." ; | |3B| : écriture hexadécimale dans le content  !"…" possible | |
|  | nocase ; | Le content n’est plus sensible à la casse |
|  | depth :12 ; | Offset jusqu’à ce qu’on arrête de checker |
|  | startwith ; | Uniquement à partir du début |
|  | offset :0 ; | A partir de quand on commence à checker |
|  | distance :1 ; | Distance relative au précédent content. |
|  |  | |