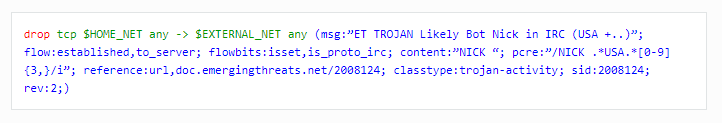
**Rules**

**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 |

|  |  |  |
| --- | --- | --- |
| **Contenu** | **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. |
|  | within :1 ; | Distance relative au précédent match |
|  | Isdataat :512 ;  Isdataat :50, relative ; |  |
|  | dsize :<number> ; | Taille du payload |
|  | rpc : |  |
|  | replace : "…" | Changement de contenu.  Checksum recalculé |
|  | pcre :"<REGEX>" ; |  |
|  | fast\_pattern ; | Le MPM (le moteur qui check plusieurs content) utilise ce content la pour établir un match avant de tester les autres contents.  Si absent, Suricata détermine le fast\_pattern à utiliser. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Flow** | **Comments** | | |
| flowbit : <opts> | set, <name> | | Set la condition |
|  | isset, <name> | | Alerte si match + la condition est set |
|  | toggle, <name> | | Inverse le set : si set, unset et vice versa |
|  | unset, <name> | |  |
|  | isnotset, <name> | |  |
|  | noalert | | Cette règle ne soulève pas d’alerte |
| flow :<direction>, <opts> | to\_client | | <direction> |
|  | to\_server | |
|  | from\_client | |
|  | from\_server | |
|  | established | |  |
|  | not\_established | |  |
|  | stateless | | Established + not established |
|  | only\_stream | | Paquets réassemblés |
|  | no\_stream | | Match paquets qui ne sont pas réassemblés uniquement |
|  | only\_frag | |  |
|  | no\_frag | |  |
| Flowint : <Opts> | Compteur d’occurrences, valeurs seuils avant alertes etc… | | |
|  | usernamecount, +, 1 ; | +1 à chaque occurence | |
|  | usernamecount, >, 5 ; | Alertes si > 5 occurences | |
| stream\_size :<server|client|both|either>, <modifier>, <number> | | | |

|  |  |
| --- | --- |
| **HTTP** | **Comments** |
| Check des différentes parties d’une trame HTTP | |

|  |  |
| --- | --- |
| **File** | **Comments** |
| filename :<string> ; |  |
| fileext :<string> ; | Extension d’un fichier |
| filestore :<direction>,<scope> ; | Stockage du fichier si la signature match |
| filemd5 :[ !]<filename> ; | Check du hash |
| filesha1 :[ !]<filename> ; |
| filesha256 :[ !]<filename> ; |
| filesize :<value> ; | >100MB|100<>200… |

|  |  |
| --- | --- |
| **Protocole** | **Comments** |
| app-layer-protocol : [ !]<protocol> ; | Ssh| !tls|failed… |
| app-layer-event :<name> ; |  |

|  |  |
| --- | --- |
| **Xbits** | **Comments** |
| xbits :<opts> | Bits stockés par Hosts ou IPs avec expiration dans le temps |

|  |  |
| --- | --- |
| **Threshold** | **Comments** |
| Threshold : type <type>, track <track>, count <N>, seconds <T>  <type> : threshold|limit|both  Threshold pour déclencher une alerte après X count, limit pour éviter le flood d’alertes  <track> : by\_src|by\_dst | |
| Detection\_filter : track <track>, count <N>, seconds <T>  Une alerte à chaque fois après que le seuil est dépassé | |

**Cas pratique :**

|  |  |  |
| --- | --- | --- |
| **Emerging Threats** | **Comments** | **Classtype** |
| App-layer-events.rules |  |  |
| Botcc.portgrouped.rules |  |  |
| Botcc.rules |  |  |
| Ciarmy.rules |  |  |
| Compromised.rules |  |  |
| Decoder-events.rules |  |  |
| Dnp3-events.rules |  |  |
| Dns-events.rules |  |  |
| Drop.rules |  |  |
| Dshield.rules |  |  |
| Emerging-activex.rules |  |  |
| Emerging-attack\_response.rules |  |  |
| Emerging-chat.rules |  |  |
| Emerging.conf |  |  |
| emerging-current\_events.rules |  |  |
| emerging-deleted.rules |  |  |
| emerging-dns.rules |  |  |
| emerging-dos.rules |  |  |
| emerging-exploit.rules |  |  |
| emerging-ftp.rules |  |  |
| emerging-games.rules |  |  |
| emerging-icmp\_info.rules |  |  |
| emerging-icmp.rules |  |  |
| emerging-imap.rules |  |  |
| emerging-inappropriate.rules |  |  |
| emerging-info.rules |  |  |
| emerging-malware.rules |  |  |
| emerging-misc.rules |  |  |
| emerging-mobile\_malware.rules |  |  |
| emerging-netbios.rules |  |  |
| emerging-p2p.rules |  |  |
| emerging-policy.rules |  |  |
| emerging-pop3.rules |  |  |
| emerging-rpc.rules |  |  |
| emerging-scada.rules |  |  |
| emerging-scan.rules |  |  |
| emerging-shellcode.rules |  |  |
| emerging-smtp.rules |  |  |
| emerging-snmp.rules |  |  |
| emerging-sql.rules |  |  |
| emerging-telnet.rules |  |  |
| emerging-tftp.rules |  |  |
| emerging-trojan.rules |  |  |
| emerging-user\_agents.rules |  |  |
| emerging-voip.rules |  |  |
| emerging-web\_client.rules |  |  |
| emerging-web\_server.rules |  |  |
| emerging-web\_specific\_apps.rules |  |  |
| emerging-worm.rules |  |  |
| files.rules |  |  |
| gen-msg.map |  |  |
| http-events.rules |  |  |
| modbus-events.rules |  |  |
| nfs-events.rules |  |  |
| ntp-events.rules |  |  |
| rbn-malvertisers.rules |  |  |
| rbn.rules |  |  |
| sid-msg.map |  |  |
| smtp-events.rules |  |  |
| stream-events.rules |  |  |
| tls-events.rules |  |  |
| tor.rules |  |  |
| unicode.map |  |  |