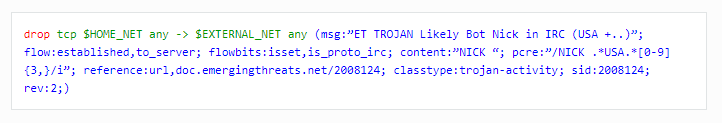
**Rules**

**Généralités :**



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

**Actions :**

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

**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 |
| 1.1.1.1/19 | Utilisation de sous réseaux possibles |
| !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 : Alerte au max N fois  Both : Le N fixe la valeur seuil avant génération d’une alerte et on alerte une seule fois durant le temps donné  <track> : by\_src|by\_dst | |
| Detection\_filter : track <track>, count <N>, seconds <T>  Threshold : Alerte lancée = reset du compteur  Detection filter : une alerte à chaque fois après que le seuil est dépassé | |

**Cas pratique :**

* Vert : Obligatoire
* Jaune: Optionnels (problèmes secondaires, infos)
* Orange : protocole spécifique
* Rouge : Osef

|  |  |  |
| --- | --- | --- |
| **Emerging Threats** | **Comments** | **Classtype** |
| Botcc.portgrouped.rules | Listes d’IPs de Bots connus  Juste IPs pas de ports dans botcc.rules  Même IPs dans botcc.portgrouped mais avec les ports, donc utiliser un des deux  1 alerte par heure maxi  Set les flowbits :   * ET.Evil * ET.BotccIP | Trojan-activity  (de l’infra vers les bad IPs) |
| Botcc.rules |
| Ciarmy.rules | Liste d’IPs des tops attaquants  <http://ciarmy.com>  1 alerte par heure maxi | Misc-attack  (des bad IPs vers l’infra) |
| Compromised.rules | Liste d’IPs compromises  1 alerte par minute maxi |
| Drop.rules | Listes d’IPs Spammers et d’IPs cybercriminels : Botnets, trojans, malwares…  <http://spamhaus.org>  1 alerte par heure maxi  Set les flowbits :   * ET.Evil * ET.DROPIP |
| Dshield.rules | Liste d’IPs des tops attaquants.  <http://dshield.org>  1 alerte par heure maxi  Set les flowbits :   * ET.Evil * ET.DshieldIP |
| Emerging-activex.rules | ActiveX | Attemped-user  Web-application-attack  Misc-attack |
| Emerging-attack\_response.rules | Attaques réussies  Id=root  Bruteforce…  Pas de post activité virus/trojan, ce sera dans la catégorie virus/trojan | All |
| Emerging-chat.rules | Chat Facebook  MSN, IRC… | Policy-violation  Misc-activity |
| emerging-current\_events.rules | Règles de test à inclure plus tard dans une autre catégorie, ou règles correspondant à, des menaces temporaires ou règles pour investiguer sur des menaces en cours | All |
| emerging-deleted.rules | Règles qui vont être supprimées | |
| emerging-dns.rules | DNS | All |
| emerging-dos.rules | DOS | Attempted-dos |
| emerging-exploit.rules | Détection d’exploits  SQL injection pas ici | Attempted-admin  Attempted-dos  Successful-dos  Web-application-attack  … |
| emerging-ftp.rules | FTP | All |
| emerging-games.rules | WoW, Starcraft…non corporate  On peut dégager |  |
| emerging-icmp\_info.rules | Relève une alerte pour chaque trame ICMP | Misc-activity  Attempted-recon |
| emerging-icmp.rules |  |
| emerging-imap.rules | IMAP | Misc-attack  Attempted-admin |
| emerging-inappropriate.rules | Sites porno donc non corporate  On peut dégager | Policy-violation |
| emerging-info.rules |  | All |
| emerging-malware.rules | Obligatoire | Trojan-activity |
| emerging-misc.rules | Others attacks not covered in others categories | All |
| emerging-mobile\_malware.rules | Android… |  |
| emerging-netbios.rules | Netbios | All |
| emerging-p2p.rules | Bitorrent, Limewire… non corporate  On peut dégager |  |
| emerging-policy.rules | Myspace, Facebook, Ebay…non corporate  On peut dégager |  |
| emerging-pop3.rules | POP3 | Attempted-admin |
| emerging-rpc.rules | RPC | All |
| emerging-scada.rules | SCADA |  |
| emerging-scan.rules | Détection scans de ports | All |
| emerging-shellcode.rules | Shellcodes  A voir parce que très noisy |  |
| emerging-smtp.rules | SMTP |  |
| emerging-snmp.rules | SNMP |  |
| emerging-sql.rules | SQL |  |
| emerging-telnet.rules | Telnet |  |
| emerging-tftp.rules | TFTP |  |
| emerging-trojan.rules | Obligatoire |  |
| emerging-user\_agents.rules |  |  |
| emerging-voip.rules | VOIP |  |
| emerging-web\_client.rules |  |  |
| emerging-web\_server.rules |  |  |
| emerging-web\_specific\_apps.rules |  |  |
| emerging-worm.rules | Vers |  |
| files.rules |  |  |
| tor.rules | Utilisation de Tor  On garde c’est suspicieux |  |
| rbn.rules | Obsolète |  |
| rbn-malvertisers.rules |  |

|  |  |  |
| --- | --- | --- |
| **EVENTS** | | |
| App-layer-events.rules | Une par connexion  Relatifs aux protocoles | Protocol-command-decode |
| Decoder-events.rules | Paquet IP invalide (CRC, trames non conformes…) | Protocol-command-decode |
| Dnp3-events.rules | DNP3 | Protocol-command-decode |
| Dns-events.rules | DNS |
| http-events.rules | Au plus une par connexion  Trame http invalide |
| modbus-events.rules | Trame Modbus invalide |
| nfs-events.rules | Trame NFS invalide |
| ntp-events.rules | Trame NTP invalide |
| smtp-events.rules | Trame SMTP invalide |
| tls-events.rules | Trame TLS invalide |
| stream-events.rules | Echange TCP invalide (+ trop de SYN…) | Protocol-command-decode |

|  |  |  |
| --- | --- | --- |
| **AUTRES** | | |
| gen-msg.map |  |  |
| sid-msg.map |  |  |
| unicode.map |  |  |