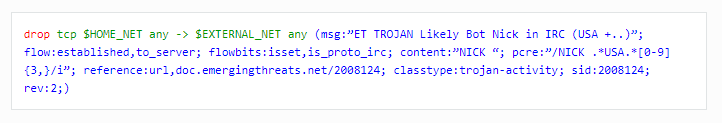
**Rules**

**Généralités :**



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

**Actions :**

|  |  |  |
| --- | --- | --- |
| **Action** | **Comment** | |
| alert | Alerte + on continue les règles suivantes | |
| reject | Mode IPS  Alerte + drop du paquet avec message d’info TCP ou ICMP indiquant une erreur | |
| drop | Mode IPS  Alerte + drop du paquet et aucun message d’erreur envoyé | |
| pass | Si match, Suricata zappe le reste des règles et aucune alerte | |
| supress gen\_id 0, sig\_id 0, track by\_src, ip X.X.X.X | | Permet de s’assurer qu’un host ne soulève aucune alerte même si ça a matché avant  Ou de faire taire une règle |

**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.

|  |  |
| --- | --- |
| **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|by\_both|by\_rule | |
| 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 :**

|  |  |  |
| --- | --- | --- |
| **Emerging Threats**  **SID range** | **Comments** | **Classtype** |
| **Règles IPs compromises**  **2 400 000 – 2 500 000**  **-**  **RESEAU** | | |
| Botcc.portgrouped.rules  2 405 000 – 2 410 000 | 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  2 404 000 – 2 410 000 |
| Ciarmy.rules  2 403 300 – 2 403 399 | Liste d’IPs des tops attaquants  <http://ciarmy.com>  1 alerte par heure maxi | Misc-attack  (des bad IPs vers l’infra) |
| Compromised.rules  2 500 000 – 2 500 040 | Liste d’IPs compromises  1 alerte par minute maxi |
| Drop.rules  2 400 001 – 2 400 032 | 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  2 402 000 | Liste d’IPs des tops attaquants.  <http://dshield.org>  1 alerte par heure maxi  Set les flowbits :   * ET.Evil * ET.DshieldIP |

|  |  |  |
| --- | --- | --- |
| **Règles violation politique d’entreprise** | | |
| Emerging-chat.rules | Chat Facebook, Gadu Gadu, ICQ  Jabber, MSN, Yahoo, Skype, AIM,  Google talk  chat IRC  Check si échanges fichiers ­| messages | Misc-activity  Not-suspicious  Policy-violation  Trojan-activity |
| emerging-games.rules | Utilisation Battle.net, WoW, TeamSpeack2, Minecraft..  + attaques sur ces produits | Attempted-admin  Misc-attack  Policy-violation |
| emerging-inappropriate.rules | Consultation sites porno  (très incomplet ^^) | Policy-violation |
| emerging-p2p.rules | Utilisation Bitorrent, Limewire, TOR…  + attaque sur ces protocoles  + trafic de infra vers Serveur P2P | Attempted-user  Policy-violation  Trojan-activity |
| emerging-policy.rules | Bordel monumental  Accès page config routeur D-Link  Bruteforce FTP admin  Connexion admin sur ports 1723 5631  Reconnaissance de services (browser…)  Connexion vers proxy  Problème versioning sécurité Java  M$ installer  Commandes AT  Ports MySQL non communs…  .exe dans URL  Utilisation du login/mdp par défaut  Flux en clair vers console…  Download ZIP  Javascript dans PDF  Connexion IRC  Scan Browser  Flux IRC sur ports non communs  Ip\_proto non commun  Ports FTP non communs  Mode configuration Cisco  Monitoring Nagios  Mdp en clair  Myspace, Facebook, Eb, Netflix…  Liens terroristes  Streaming  Installation DLL  IP tracking via javascript  Requête DNS vers sites .onion  Commande powershell via SMB  Utilisation d’un proxy  Invalid login  Ports SSL non communs  Pas d’SSL avec Exchange  Accès JBOSS depuis exterieur | Attempted-admin  Attempted-recon  Attempted-user  Bad-unknown  Default-login-attempt  Misc-activity  Misc-attack  Network-scan  Non-standard-protocol  Not-suspicious  Policy-violation  Protocol-command-decode  Successful-admin  Successful-recon-limited  Suspicious-filename-detect  Trojan-activity  Unknown  Unsuccessful-user  Unusual-client-port-connection  Web-application-activity  Web-application-attack |
| tor.rules | Utilisation des relais connus de Tor  Inspection des IPs | Misc-attack  (des Relais vers IPs infra) |

|  |  |  |
| --- | --- | --- |
| **Règles protocoles spécifiques** | | |
| Emerging-activex.rules | ActiveX | Attempted-admin  Attemped-user  Misc-attack  Successful-user  Web-application-attack |
| emerging-dns.rules | DNS  Overflow, exploits  Infos sur DNS  DNS tunneling… | Attempted-admin  Attempted-recon  Bad-unknown  Not-suspicious  Policy-violation  Trojan-activity |
| emerging-ftp.rules | FTP | Attempted-admin  Attempted-dos  Attempted-recon  Attempted-user  Bad-unknown  Denial-of-service  Misc-activity  Misc-attack  Not-suspicious  Protocol-command-decode  String-detect  Suspicious-filename-detect  Suspicious-login  Trojan-activity  unknown |
| emerging-imap.rules | IMAP | Attempted-admin  Attempted-user  Misc-attack |
| emerging-netbios.rules | Netbios | Attempted-admin  Attempted-dos  Attempted-recon  Attempted-user  Bad-unknown  Denial-of-service  Misc-activity  Misc-attack  Protocol-command-decode  Suspicious-filename-detect  Unsuccessful-user |
| emerging-pop3.rules | POP3 | Attempted-admin  Misc-attack |
| emerging-scada.rules | SCADA | Attempted-dos  Attempted-user  Denial-of-service |
| emerging-smtp.rules | SMTP | Attempted-admin  Misc-attack |
| emerging-snmp.rules | SNMP | Attempted-admin  Attempted-recon  Attempted-user  Bad-unknown  Misc-activity  Misc-attack  Not-suspicious  Protocol-command-decode  Suspicious-filename-detect  Suspicious-login |
| emerging-sql.rules | SQL | Attempted-user  Bad-unknown  Misc-activity  Misc-attack  Protocol-command-decode  Shellcode-detect  Suspicious-filename-detect  Unsuccessful-user  Web-application-attack |
| emerging-telnet.rules | Telnet | Attempted-admin  Bad-unknown  Not-suspicious  Suspicious-filename-detect  Suspicious-login |
| emerging-tftp.rules | TFTP | Attempted-admin  Attempted-dos  Bad-unknown  Policy-violation  Successful-admin |
| emerging-voip.rules | VOIP | Attempted-dos  Attempted-recon  Attempted-user  Misc-activity  Misc-attack |

|  |  |  |
| --- | --- | --- |
| **Règles Malwares/Exploits/…** | | |
| Emerging-attack\_response.rules | Attaques réussies  Id=root  Bruteforce…  Pas de post activité virus/trojan, ce sera dans la catégorie virus/trojan | Attempted-admin  Attempted-recon  Attempted-user  Bad-unknown  Misc-activity  Policy-violation  Protocol-command-decode  String-detect  Successful-admin  Successful-recon-limited  Successful-user  Trojan-activity  Web-application-activity  Web-application-attack |
| 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 | Attempted-admin  Attempted-dos  Attempted-recon  Attempted-user  Bad-unknown  Misc-activity  Not-suspicious  Policy-violation  Successful-admin  Successful-user  Trojan-activity  Web-application-activity  Web-application-attack |
| emerging-dos.rules | DOS | Attempted-dos  Attempted-user  Bad-unknown  Denial-of-service  Not-suspicious  Trojan-activity  Web-application-attack |
| emerging-exploit.rules | Détection d’exploits  SQL injection pas ici | Attempted-admin  Attempted-dos  Attempted-recon  Attempted-user  Bad-unknown  Default-login-attempt  Denial-of-service  Misc-activity  Misc-attack  Non-standard-protocol  Not-suspicious  Rpc-portmap-decode  Shellcode-detect  Successful-admin  Successful-dos  Successful-user  Suspicious-filename-detect  Suspicious-login  System-call-detect  Trojan-activity  Web-application-activity  Web-application-attack |
| emerging-malware.rules | Obligatoire | Attempted-recon  Bad-unknown  Misc-activity  Misc-attack  Non-standard-protocol  Policy-violation  Trojan-activity |
| emerging-misc.rules | Others attacks not covered in others categories | Attempted-admin  Attempted-dos  Attempted-user  Bad-unknown  Misc-activity  Misc-attack  Network-scan  Non-standard-protocol  Protocol-command-decode  String-detect  unknown  Unsuccessful-user  Web-application-activity |
| emerging-mobile\_malware.rules | Android… | Policy-violation  Trojan-activity |
| emerging-rpc.rules | RPC | Attempted-admin  Attempted-recon  Bad-unknown  Misc-attack  Rpc-portmap-decode  Unsuccessful-user |
| emerging-scan.rules | Détection scans de ports | Attempted-admin  Attempted-dos  Attempted-recon  Attempted-user  Bad-unknown  Default-login-attempt  Misc-activity  Misc-attack  Network-scan  Not-suspicious  Protocol-command-decode  Successful-admin  Successful-login  Trojan-activity  Unsuccessful-user  Web-application-activity  Web-application-attack |
| emerging-shellcode.rules | Shellcodes  A voir parce que très noisy | Bad-unknown  Shellcode-detect  System-call-detect  Trojan-activity |
| emerging-trojan.rules | Obligatoire | Attempted-admin  Attempted-dos  Attempted-user  Bad-unknown  Denial-of-service  Misc-activity  Not-suspicious  Policy-violation  Protocol-command-decode  Successful-admin  Successful-recon-limited  Successful-user  Suspicious-filename-detect  Trojan-activity  unknown  Web-application-attack |
| emerging-web\_client.rules |  | Attempted-admin  Attempted-dos  Attempted-recon  Attempted-user  Bad-unknown  Misc-activity  Misc-attack  Not-suspicious  Protocole-command-decode  Trojan-activity  Web-application-activity  Web-application-attack |
| emerging-web\_server.rules |  | Attempted-admin  Attempted-dos  Attempted-recon  Attempted-user  Bad-unknown  Misc-activity  Misc-attack  Network-scan  Policy-violation  Successful-admin  Successful-recon-limited  Successful-user  Trojan-activity  Web-application-activity  Web-application-attack |
| emerging- web\_specific\_apps.rules |  | Attempted-admin  Attempted-dos  Attempted-recon  Attempted-user  Misc-activity  Misc-attack  Successful-recon-largescale  Trojan-activity  Web-application-activity  Web-application-attack |
| emerging-worm.rules | Vers | Misc-attack  Trojan-activity |
| files.rules |  | - |

|  |  |  |
| --- | --- | --- |
| **Règles Logging** | | |
| emerging-icmp\_info.rules | Logging des Codes ICMP  Traceroute via ICMP | Attempted-recon  Bad-unknown  Misc-activity |
| emerging-icmp.rules | Paquet ICMP de grande taille  Code ICMP non définie… |
| emerging-info.rules | Requête sur certains domaines  Certains téléchargements  … | Attempted-admin  Attempted-recon  Attempted-user  Bad-unknown  Misc-activity  Misc-attack  Network-scan  Not-suspicious  Policy-violation  Protocol-command-decode  Shellcode-detect  Successful-recon-limited  Trojan-activity |
| emerging-user\_agents.rules |  | Attempted-recon  Bad-unknown  Misc-activity  Policy-violation  Trojan-activity |

|  |  |  |
| --- | --- | --- |
| **Règles obsolètes** | | |
| emerging-deleted.rules | Règles qui vont être supprimées | |
| rbn.rules | Obsolète |  |
| rbn-malvertisers.rules |  |

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

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

**Classtypes :**

|  |  |
| --- | --- |
| **Classtype** | **Comments** |
| Attempted-admin | Buffer-overflow  Bruteforce  Connexion Admin  Accès page config d’un routeur |
| Attempted-dos |  |
| Attempted-recon | Reconnaissance de services  Traceroute dans ICMP |
| Attempted-user | Buffer-overflow  Connexion infra vers proxy |
| Bad-unknown | Problème versioning sécurité Java  M$ installer  Commandes AT  Ports MySQL non communs…  .exe dans URL |
| Default-login-attempt | Utilisation du login/mdp par défaut |
| Denial-of-service |  |
| Icmp-event | ? |
| Inappropriate-content | ? |
| Misc-activity | Utilisation de protocoles IRC  Flux en clair vers console…  Download ZIP  Javascript dans PDF |
| Misc-attack | Traffic d’IPs répudiées vers l’infrastructure  Exécution de code  TOR vers infra |
| Network-scan | Scan Browser |
| Non-standard-protocol | Flux IRC sur ports non communs  Ip\_proto non commun  Ports FTP non communs |
| Not-suspicious | Connexion à des ports IRC  Mode configuration Cisco  Monitoring Nagios |
| Policy-violation | Echanges messages ou fichiers Facebook, MSN etc… (chat)  Utilisation jeux vidéo  Consultation sites porno  Utilisation P2P  Mdp en clair  Myspace, Facebook, Eb, Netflix…  Liens terroristes  Streaming  … |
| Protocol-command-decode |  |
| Rpc-portmap-decode |  |
| Shellcode-detect |  |
| String-detect |  |
| Successful-admin | Installation DLL |
| Successful-dos |  |
| Successful-recon-largescale |  |
| Successful-recon-limited | IP tracking via javascript |
| Successful-user |  |
| Suspicious-filename-detect |  |
| Suspicious-login |  |
| System-call-detect |  |
| Tcp-connection | ? |
| Trojan-activity | Traffic de l’infrastructure vers des IPs répudiées  Infra répond sa version de chat Gadu Gadu, vers un serveur P2P  Requête DNS vers sites .onion  Commande powershell via SMB |
| Unknown |  |
| Unsuccessful-user | Invalid login |
| Unusual-client-port-connection | Ports SSL non communs |
| Web-application-activity | Pas d’SSL avec Exchange |
| Web-application-attack | Accès JBOSS depuis exterieur |