IDS - Suricata

Aurélien Monnet-Paquet

www.inria.fr

17 Mars 2016

Qu'est ce qu'un IDS ?

- Systèmes de détection d'intrusion
- Écoute le réseau de manière furtive afin de repérer des activités suspectes

Qu'est ce qu'un IDS ?

- Systèmes de détection d'intrusion
- Écoute le réseau de manière furtive afin de repérer des activités suspectes
- Placement de l'IDS au niveau du routeur de sortie/d'entrée du réseau

Qu'est ce qu'un IDS ?

- Systèmes de détection d'intrusion
- Écoute le réseau de manière furtive afin de repérer des activités suspectes
- Placement de l'IDS au niveau du routeur de sortie/d'entrée du réseau
- Et la concurrence ? Snort Suricata Bro ...

La différence avec un IPS ?

- Systèmes de prévention d'intrusion
- Pas discret, facilement détectable

La différence avec un IPS ?

- Systèmes de prévention d'intrusion
- Pas discret, facilement détectable
- Bloque tout ce qui parait infectieux, y compris le trafic légitime

La différence avec un IPS ?

- Systèmes de prévention d'intrusion
- Pas discret, facilement détectable
- Bloque tout ce qui parait infectieux, y compris le trafic légitime
- Pas la même méthode d'analyse qu'en mode IDS

But de Suricata (2008)

- Apporter de nouvelles technologies aux IDS :
  - Performance : Le multi-threading
  - Accélération matérielle (par GPU)
- Support d'IPv6 natif
- Open source
- Disponible sur Linux / MAC / Windows
- Supporte presque toutes les signatures de snort

Snort et Bro

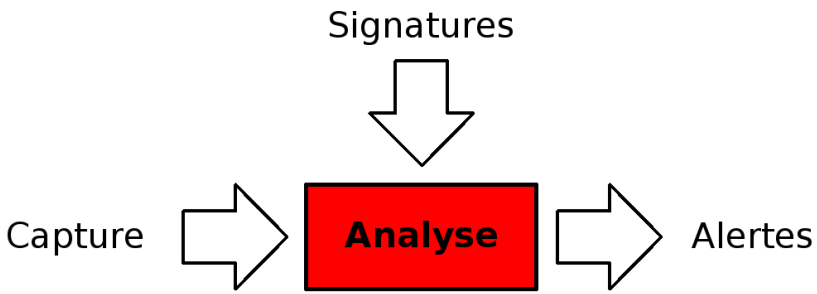
- Snort
  - Développé par Sourcefire
  - Fonctionnellement équivalent à Suricata
  - Compatibilité Snort / Suricata
  - Concurrence directe

Snort et Bro

- Snort
  - Développé par Sourcefire
  - Fonctionnellement équivalent à Suricata
  - Compatibilité Snort / Suricata
  - Concurrence directe
- Bro
  - Orientation capture
  - Études statistiques

Fonctionnement

- Lève une alerte mais ne bloque pas le flux (rôle de l'IPS)
- Travail avec un flux de données
- Reconstruction du flux : TCP => perte/renvoi/ordre
- La réception d'un ACK déclenche l'analyse des données.



Fonctionnement des règles de matching

alert http any any → any any (msg :"" ; content :"inria.fr" ;)

Actions :

1. pass
2. drop
3. reject
4. alert

Fonctionnement des règles de matching

alert http any any → any any (msg :"" ; content :"inria.fr" ;)

Protocole :

- tcp / udp
- ip
- icmp

Fonctionnement des règles de matching

alert http any any → any any (msg :"" ; content :"inria.fr" ;)

Source/Destination Port :

- 128.93.162.84 80 → 192.168.17.218 any
- $*EXTERNAL\_NET$ any <> $*HOME\_NET$ any

Fonctionnement des règles de matching

alert http any any → any any (msg :"" ; content :"inria.fr" ;)

Motif

Fonctionnement des règles de matching

alert http any any → any any (msg :"" ; content :"inria.fr" ;)

Autres paramètres :

- msg :"Connexion établie depuis le site www.inria.fr"
- http_uri, http_method, http_header, http_cookie ...
- flow :established,to_server ; to_client ; nocase ; ...

Flowint

Initialisation d'une variable

alert tcp any any ⇒ any any (msg : "Start a login count" ; content : "login failed" ; flowint : loginfailed, notset ; flowint : loginfail, =, 1 ; sid :999997 ; rev :5 ;)

Flowint

Initialisation d'une variable

alert tcp any any ⇒ any any (msg : "Start a login count" ; content : "login failed" ; flowint : loginfailed, notset ; flowint : loginfail, =, 1 ; sid :999997 ; rev :5 ;)

Incrémentation d'une variable

alert tcp any any ⇒ any any (msg : "Counting Logins" ; content : "login failed" ; flowint : loginfailed, isset ; flowint : loginfail, +, 1 ;)

Suricata et LibHtp

Capable de décoder des flux compressés par Gzip

Page non compressée

alert http 128.93.162.84 any -> any any (msg :"LOCAL Flux depuis inria.fr mot clé (http)" ; flow :to_client ; content :"Inria recrute" ; nocase ; sid :999992 ; rev :5 ;)

Page compressée

alert http any any -> any any (msg :"LOCAL Flux depuis UGA mot clé (http)" ; flow :to_client ; content :"est astrophysicien" ; http_server_body ; nocase ; sid :999990 ; rev :5 ;)

Décompression de fichiers

Extraction et inspection des fichiers compressé.

Règle de base

alert http any any -> any any (msg :"FILE store all" ; filestore ; sid :1 ; rev :1 ;)