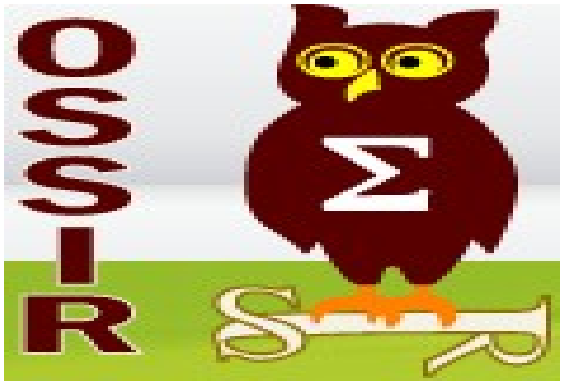
O.S.S.I.R. rdv du 11 mai 2010

Présentation du projet « Suricata »

`Nouveau moteur de Détection et de Protection d'Intrusion Réseau Open Source`



Franck Debieve
rmkml@free.fr

Sommaire

=>Suricata (wikipedia) est une petite espèce de mangouste, mammifère carnivore vivant dans le sud de l'Afrique.

-Présentation du projet et de ses principaux membres

-Points clefs du projet

-Futurs évolutions

-Status du projet

-Contacts

Présentation du projet (1)

Le projet « Suricata » à démarrer mi 2008.
C'est un projet sous licence GPLv2.
La première version disponible du code source (v0.8.0) est apparue le 31 déc 2009.

Les sociétés ou organisations suivantes supportent le projet:
-Navy's Space and Naval Warfare Systems Command
-Homeland Open Security Technology
-Bivio Networks
-Everis
-Mammoth Law Group
-EdenWall Technologies
-Endace
-Kerio
-Nitro Security
-Breach Securit Labs

=> Certaines de ces sociétés sont des acteurs connus dans le monde « Snort »

Présentation du projet (2)

Les personnes suivantes supportent également le projet Suricata:

-Matt Jonkman (bleeding rules, maintenant Emerging Threat)

-Luca Deri (ntop, PFRing) 

-Jennifer Steffens (ex directeur Sourcefire)

-Dr. Jose Nazario (Arbor Networks)

-Marc Norton (ex developpeur pour Snort/Sourcefire)

-Victor Julien (developpeur InfoSec Community)

-Will Metcalf (mainteneur du projet snort_inline)

Points clef du projet (1)

-Alternative à Snort! (et Bro)
-Support du multi-threading dés le début du projet
(en attendant Snort v3!)
-IDS mode: Détection d'intrusion réseau
-IPS mode: Blocage ou Prévention des intrusions
via netfilter/nfQueue sous linux ou ipfw/divert freebsd
-Support du protocole HTTP via la librairie HTP
-Compatibilité des signatures avec Snort 2.8.6*
-Support PFRing natif
-Auto détection des protocoles les plus connues
(http,ftp,smtp,https,ssh,imap,msn,smb...)
-support des cartes Dag d'Endace

* Toutes les nouvelles options Snort sont en cours de portage

Points clef du projet (2)

-Support alpha CUDA (GPU)
-Support IPv6 (compilé par défaut!)
-Support Libnet (injection de packet)

-FlowInt (comme flowbit mais de manière globale et pas seulement pour le même stream!)
-Sortie des alertes aux formats Syslog/Fast/Unified2/Prelude
-Host et HTP Specific policy (définition spécifique du ré-assemblage sur une ip ou pour un serveur web)
-Le langage de configuration (yaml) permet des vérifications de configuration plus stricte que snort (par exemple offset,distance,reference keywords)

Exemples

Les nouvelles options de configuration permettent d'écrire des signatures sur plusieurs lignes:

```
alert tcp any any → any $HTTP_PORTS \
 (msg: «Suricata »; flow:to_server,established; \
  content: «x»;...
```

Le nouveau détecteur de protocoles permet d'écrire des signatures sans préciser le port:

```
alert http any any → any any...
```

Valables pour les protocoles http,ftp,smtp,https,ssh,imap...

Exemple de signature avec flowint:

```
alert tcp any any -> any any (msg:"More than Five
Usernames!"; content:"jonkman"; \
flowint: usernamecount, +, 1; flowint:usernamecount, >, 5;)
```

Futurs du projet

-Suricata bientôt disponible pour les plateformes Windows
-Une interface web de configuration
-Evolution du Support des GPU via CUDA
-IP reputation et GeoIP
-évolution des algorithmes de pattern matching
-nouvelle base contenant les URL Hostile
-de nouveau protocole de détection automatique
-FlowVar
-Passive SSL Decryption (multithreading et/ou cuda et/ou networkprocessor)
-support de la Virtualisation (Suricata est un logiciel donc facilement virtualisable)
-Fast Regular Expression (par exemple via CUDA ou via des network processeurs)
-Décompression des réponses web (performant via le multithreading!)

Google code

Status / Feedback du projet

Depuis la première version publique (début 2010), le projet avance vite.

La version 0.8.2 intègre la première version du code supportant CUDA et de la puissance de traitement des GPU.

La première version 0.9.0 Release Candidate (RC) à été annoncée pour début Mai 2010, mais elle aura un peu de retard.

La première version stable est annoncée pour Juillet-Aout.

Contacts

Franck Debieve: rmkml@free.fr

Projet Suricata: http://www.openinfosecfoundation.org/

Projet CUDA: http://www.nvidia.fr/object/cuda.html

Signatures pour Suricata: http://www.emergingthreats.net/
(également pour Bro + Snort)