Technicien Supérieur Gestionnaire
de Ressources Informatiques
et Réseaux

How to protect your system

Anti Malware Corner

'The Definitive Guide'

O RLY?

L.Marchal

Table des matières

Malware corner

Ce document regroupe plusieurs utilitaires permettant de :

monitorer son système avec :

Lynis et/ou RK-Hunter

Dont le code est disponible sur gitHub :
https://github.com/CISOfy

Distribué par Cisofy.

Toujours au niveau système il existe CHKROOKIT .

Monitorer son réseau avec l'IDS SURICATA

Malware detector qui utilise le moteur Clam-AV l'anti virus utilisé sous Mac OS, et gnu/Linux d'une manière générale.

Disponible au téléchargement ainsi que sur GitHub.

http://www.clamav.net/downloads

https://github.com/vrtadmin

A noté qu'il y a une section SNORT (Un autre IDS de marque CISCO)

Les menaces informatique ont évolués, à l'époque les petits malins s'amusaient à rependre des vers, détruire des disques, simplement pour démontrer qu'ils étaient capable de le faire.

Par la suite ils ont trouvés plus intelligent de s'introduire dans vos systèmes et réseaux.

1. De ce fait ils prennent possession de votre machine afin qu'elle lui obéisse.
2. Ce que l'on nomme des ROOTKIT

Aussi existe-t-il des produits comme Lynis, RK-Hunter et CHKROOTKIT, qui vont vérifier la présence de certains fichiers de configuration, vous signifiant quels fichiers il serait intéressant de modifier.

Lynis par exemple va générer une somme de contrôle permettant alors de faire une comparaison avec une somme d'origine, vous permettant alors de constater les changements dans votre système.

Lynis

outil d'audit de sécurité pour les systèmes à base Unix

Lynis est un outil d'audit pour Unix. Il parcourt la configuration du système et crée un résumé des informations système et des problèmes de sécurité, utilisable par des auditeurs professionnels. Il peut aider à des audits automatisés.

Lynis peut être utilisé en plus d'autres logiciels comme les analyseurs de sécurité, les outils de mesures de performance du système et les outils de réglage fin. Lynis va auditer tout le système, en cherchant la présence, l'absence de fichier ou module, d'application, et donne un rapport en fonction des critères de recherches.

Lynis s'execute sur votre machine sans avoir besoin de l'installer.

Lien vers le site de cisofy.

Usage

Le scann est assez long et vous donnera énormément d'information sur votre systèm et sa configuration.

```
lynis -c
```

Aperçu du résultat du scan.

```
Follow-up:
  ----------------------------
  - Check the logfile for more details (less /var/log/lynis.log)
  - Read security controls texts (https://cisofy.com)
  - Use --upload to upload data (Lynis Enterprise users)

================================================================================
  Lynis Scanner (details):

  Hardening index : 63 [############        ]
  Tests performed : 207
  Plugins enabled : 1

  Lynis Modules:
  - Heuristics Check [NA] - Security Audit [V]
  - Compliance Tests [X] - Vulnerability Scan [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================
  Notice: Lynis update available
  Current version : 200    Latest version : 211
================================================================================
  Tip: Disable all tests which are not relevant or are too strict for the
       purpose of this particular machine. This will remove unwanted suggestions
       and also boost the hardening index. Each test should be properly analyzed
       to see if the related risks can be accepted, before disabling the test.
================================================================================


  Lynis 2.0.0
  Auditing, hardening and compliance for BSD, Linux, Mac OS and Unix
  Copyright 2007-2015 - CISOfy, https://cisofy.com
  Enterprise support and plugins available via CISOfy
================================================================================
```

CRON

Ajoutez ce script dans /etc/cron.daily

Nommez le lynis

Le rendre excutable chmod +x lynis, et pensez à créer les répertoire de log :

mkdir /var/log/lynis

mkdir /usr/local/lynis

```
#!/bin/sh
AUDITOR="automated"
DATE=$(date +%Y%m%d)
HOST=$(hostname)
LOG_DIR="/var/log/lynis"
REPORT="$LOG_DIR/report-${HOST}.${DATE}"
DATA="$LOG_DIR/report-data-${HOST}.${DATE}.txt"

cd /usr/local/lynis
./lynis -c --auditor "${AUDITOR}" --cronjob > ${REPORT}
mv /var/log/lynis-report.dat ${DATA}

# The End
```

rk-hunter

Lien vers le site de rk-hunter.

scanner de rootkit, porte dérobée, renifleur et exploit

Rootkit Hunter analyse les systèmes pour détecter les rootkits, portes dérobées, renifleurs et exploits connus et inconnus.

Il vérifie :

- - les changements de hachage MD5 ;
- - les fichiers couramment créées par les rootkits ;
- - les exécutables avec des permissions de fichiers anormales ;
- - les chaînes de caractères suspectes dans les modules du noyau ;
- - les fichiers cachés dans les répertoires système ;

et il peut éventuellement effectuer des analyses dans les fichiers.

Utiliser rkhunter seul ne garantit pas que le système n'est pas compromis. L'exécution de tests supplémentaires, tels que chkrootkit, est recommandé.

Installation

Pour l'installer

```
>~ sudo apt-get install rkhunter
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  bsd-mailx exim4-base exim4-config exim4-daemon-light iproute liblockfile-bin
liblockfile1 unhide
Paquets suggérés :
  eximon4 exim4-doc-html exim4-doc-info spf-tools-perl swaks tripwire libdigest-
whirlpool-perl powermgmt-base
Paquets recommandés :
  mailx default-mta mail-transport-agent
Les NOUVEAUX paquets suivants seront installés :
  bsd-mailx exim4-base exim4-config exim4-daemon-light iproute liblockfile-bin
liblockfile1 rkhunter unhide
```

```
Creating config file /etc/default/rkhunter with new version
[ Rootkit Hunter version 1.4.2 ]
File created: searched for 175 files, found 145
Paramétrage de exim4-config (4.84-8+deb8u2) ...
Adding system-user for exim (v4)
Paramétrage de exim4-base (4.84-8+deb8u2) ...
exim: DB upgrade, deleting hints-db
insserv: warning: script 'unbound' missing LSB tags and overrides
Paramétrage de exim4-daemon-light (4.84-8+deb8u2) ...
Paramétrage de bsd-mailx (8.1.2-0.20141216cvs-2) ...
```

```
update-alternatives: utilisation de « /usr/bin/bsd-mailx » pour fournir
« /usr/bin/mailx » (mailx) en mode automatique
Paramétrage de iproute (1:3.16.0-2) ...
Paramétrage de unhide (20121229-1+b1) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.19-18+deb8u1) ...
Traitement des actions différées (« triggers ») pour systemd (215-17+deb8u2) ...
Traitement des actions différées (« triggers ») pour rkhunter (1.4.2-0.4) ...
[ Rootkit Hunter version 1.4.2 ]
```

Update

Le mettre à jour :

```
rkhunter --update
```

```
System checks summary
=====================

File properties checks...
       Files checked: 147
       Suspect files: 1

Rootkit checks...
       Rootkits checked : 379
      Possible rootkits: 0

Applications checks...
      All checks skipped

The system checks took: 1 minute and 16 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

Usage

`rkhunter --check --skip-keypress -report-warnings-only`

Cette commande est très pratique, elle va vous eviter de taper entrer pour poursuivre le test, mais vous indiquera également ce que le test à découvert.
Bon parfois il ne faut pas trop s'inquiéter…

```
>~ rkhunter --check --skip-keypress -report-warnings-only
Warning: The command '/sbin/chkconfig' has been replaced by a script: /sbin/chkconfig:
Perl script, ASCII text executable
Warning: Suspicious file types found in /dev:
                /dev/shm/pulse-shm-1439826070: data
                /dev/shm/pulse-shm-967362969: data
                /dev/shm/pulse-shm-3618364688: data
                /dev/shm/PostgreSQL.1804289383: data
Warning: Hidden directory found: /etc/.java
```

Le fichier de configuration se trouve dans `/etc/rkhunter.conf`, vous pouvez y configurer, entre autre, votre adresse mail pour recevoir les alertes.

rkhunter peut générer des faux positifs, vous pouvez trouver dans la documentation d'Ubuntu comment l'éviter.

Version

Vérifiez la version avec :

`rkhunter --versioncheck`

```
>~ rkhunter --versioncheck
[ Rootkit Hunter version 1.4.2 ]

Checking rkhunter version...
  This version  : 1.4.2
  Latest version: 1.4.2
```

Config

SSH

Permet de checker si root peut se connecter en SSH (J'espère que NO!!!)

```
# The following option is checked against the SSH configuration file
# 'PermitRootLogin' option. A warning will be displayed if they do not match.
# However, if a value has not been set in the SSH configuration file, then a
# value here of 'unset' can be used to avoid warning messages.
#
# The default value is 'no'.
#
ALLOW_SSH_ROOT_USER=no
```

```
# This setting tells rkhunter the directory containing the SSH configuration
# file. This setting will be worked out by rkhunter, and so should not
# usually need to be set.
#
# This option has no default value.
#
SSH_CONFIG_DIR=/etc/ssh
```

Répertoire caché java

RKHUNTER n'apprécie pas les répertoires cachés, pourtant il en faut, aussi il faut signaler à RKHUNTER quel répertoire vous autorisez.

```
# Allow the specified hidden directory to be whitelisted.
#
# This option may be specified more than once, and may use wildcard characters.
#
# The default value is the null string.
#
ALLOWHIDDENDIR=/etc/.java
```

Usage

rkhunter -c

RKHUNTER va alors vérifier l'ensemble de vos répertoires à la recherche d'un rootkit.

Rkhunter est automatiquement ajouté au cron.daily

Maldet

Malware detector (https://www.rfxn.com/projects/linux-malware-detect/), son travail consiste à rechercher les malware en se basant sur la base de données virale maintenu par ClamAV le moteur anti virus sous Gnu/Linux, normalement également présent dans les MacOS.

Recupération

```
>~ wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
--2016-03-06 23:06:32--  http://www.rfxn.com/downloads/maldetect-current.tar.gz
Résolution de www.rfxn.com (www.rfxn.com)… 129.121.132.46
Connexion à www.rfxn.com (www.rfxn.com)|129.121.132.46|:80… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 1135368 (1,1M) [application/x-gzip]
Sauvegarde en : « maldetect-current.tar.gz »

maldetect-current.t 100%[====================>]   1,08M   529KB/s   ds 2,1s

2016-03-06 23:06:35 (529 KB/s) — « maldetect-current.tar.gz » sauvegardé
[1135368/1135368]

>~ tar xfz maldetect-current.tar.gz

>~ cd maldetect-*

># ./install.sh
```

Installation

```
>~ sudo ./install.sh
Created symlink from /etc/systemd/system/multi-user.target.wants/maldet.service to
/usr/lib/systemd/system/maldet.service.
Linux Malware Detect v1.5
                       (C) 2002-2015, R-fx Networks <proj@r-fx.org>
                       (C) 2015, Ryan MacDonald <ryan@r-fx.org>
This program may be freely redistributed under the terms of the GNU GPL

installation completed to /usr/local/maldetect
config file: /usr/local/maldetect/conf.maldet
exec file: /usr/local/maldetect/maldet
exec link: /usr/local/sbin/maldet
exec link: /usr/local/sbin/lmd
cron.daily: /etc/cron.daily/maldet
maldet(27173): {sigup} performing signature update check...
maldet(27173): {sigup} local signature set is version 2016030514389
maldet(27173): {sigup} latest signature set already installed
```

Update

```
>~ sudo maldet -u
Linux Malware Detect v1.5
                       (C) 2002-2015, R-fx Networks <proj@rfxn.com>
                       (C) 2015, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(27262): {sigup} performing signature update check...
maldet(27262): {sigup} local signature set is version 2016030514389
maldet(27262): {sigup} latest signature set already installed
```

Pour affiner vos réglages, avoir des informations par mail, configurer la mise en quarantaine, le fichier de configuration se trouve dans

/usr/local/maldetect/conf.maldet
ajouter la base de signatures de MalDet : Clamav :

Il est possible de rajouter la base de signatures de maldet à clamav, ce qui permet de scanner une seule fois avec les deux bases de signatures. Après avoir installé maldet, vous pouvez faire la manipulation suivante :

```
:/var/lib/clamav# rm /var/lib/clamav/rfxn.hdb
:/var/lib/clamav# ln -s /usr/local/maldetect/sigs/rfxn.ndb /var/lib/clamav/rfxn.ndb
:/var/lib/clamav# rm /var/lib/clamav/rfxn.ndb
:/var/lib/clamav# ln -s /usr/local/maldetect/sigs/rfxn.ndb /var/lib/clamav/rfxn.ndb
:/var/lib/clamav# clamscan --recursive --infected --log="/var/log/clamscan"

----------- SCAN SUMMARY -----------
Known viruses: 4300040
Engine version: 0.98.7
Scanned directories: 1
Scanned files: 4
Infected files: 0
Data scanned: 0.38 MB
Data read: 176.30 MB (ratio 0.00:1)
Time: 6.153 sec (0 m 6 s)
```

Vous pouvez utiliser la commande suivante pour lancer un scan, --recursive permet de descendre dans l'arborescence, --infected permet de n'afficher que les résultats positifs lors du scan pour éviter une sortie particulièrement verbeuse, et --log permet de définir un fichier ou le résultat du scan sera écrit :

```
clamscan --recursive --infected --log="/var/log/clamscan"
```

Usage

Pour l'instant maldet n'est pas lancé au démarrage nous allons donc le lancer manuellement.

Nous constatons également que malware detector utilise le moteur antiviral ClamAV: l'anti virus qui sert de base à plusieurs anti virus commerciaux; alors autant choisir l'originale. De plus c'est également l'anti virus par défaut des systèmes MacOS;
ainsi que nombres de serveur de mail.

```
sudo /usr/local/sbin/maldet -a
Linux Malware Detect v1.5
                        (C) 2002-2015, R-fx Networks <proj@rfxn.com>
                        (C) 2015, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(2000): {scan} signatures loaded: 10824 (8909 MD5 / 1915 HEX / 0 USER)
maldet(2000): {scan} building file list for /home, this might take awhile...
maldet(2000): {scan} setting nice scheduler priorities for all operations: cpunice 19 ,
ionice 6
maldet(2000): {scan} file list completed in 3s, found 139060 files...
maldet(2000): {scan} found clamav binary at /usr/bin/clamscan, using clamav scanner
engine...
maldet(2000): {scan} scan of /home (139060 files) in progress...
maldet(2000): {scan} processing scan results for hits: 2 hits 0 cleaned
maldet(2000): {scan} scan completed on /home: files 139060, malware hits 2, cleaned hits
0, time 249s
maldet(2000): {scan} scan report saved, to view run: maldet --report 160315-0859.2000
maldet(2000): {scan} quarantine is disabled! set quarantine_hits=1 in conf.maldet or to
quarantine results run: maldet -q 160315-0859.2000
maldet(2000): {alert} sent scan report to
```

Ca tombe bien

Malware detector nous explique comment accéder au rapport

```
>~ sudo maldet --report 160315-0859.2000
[sudo] password for xtbushido:
Linux Malware Detect v1.5
                        (C) 2002-2015, R-fx Networks <proj@rfxn.com>
                        (C) 2015, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2
```

Rapport

```
GNU nano 2.2.6                          Fichier :
/usr/local/maldetect/sess/session.160315-0859.2000

HOST:      gally
SCAN ID:   160315-0859.2000
STARTED:   mars 15 2016 08:59:27 +0100
COMPLETED: mars 15 2016 09:03:36 +0100
ELAPSED:   249s [find: 3s]

PATH:          /home
TOTAL FILES:   139060
TOTAL HITS:    2
TOTAL CLEANED: 0

WARNING: Automatic quarantine is currently disabled, detected threats are still
accessible to users!
To enable, set quarantine_hits=1 and/or to quarantine hits from this scan run:
/usr/local/sbin/maldet -q 160315-0859.2000

FILE HIT LIST:
{HEX}gzbase64.inject.unclassed.15  :  /home/xtbushido/maldetect-current.tar.gz
{HEX}gzbase64.inject.unclassed.15  :  /home/xtbushido/maldetect-
1.5/files/clean/gzbase64.inject.unclassed
================================================
Linux Malware Detect v1.5 < proj@rfxn.com >
```

Quarantaine

```
>~ sudo /usr/local/sbin/maldet -q 160315-0859.2000
Linux Malware Detect v1.5
                        (C) 2002-2015, R-fx Networks <proj@rfxn.com>
                        (C) 2015, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(19881): {quar} malware quarantined from '/home/xtbushido/maldetect-
current.tar.gz' to '/usr/local/maldetect/quarantine/maldetect-current.tar.gz.859127872'
maldet(19881): {quar} malware quarantined from '/home/xtbushido/maldetect-
1.5/files/clean/gzbase64.inject.unclassed' to
'/usr/local/maldetect/quarantine/gzbase64.inject.unclassed.2818915906'
```

Apres la quarantaine

```
>~ sudo /usr/local/sbin/maldet -q 160315-0859.2000
Linux Malware Detect v1.5
                        (C) 2002-2015, R-fx Networks <proj@rfxn.com>
                        (C) 2015, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(19881): {quar} malware quarantined from '/home/xtbushido/maldetect-
current.tar.gz' to '/usr/local/maldetect/quarantine/maldetect-current.tar.gz.859127872'
maldet(19881): {quar} malware quarantined from '/home/xtbushido/maldetect-
1.5/files/clean/gzbase64.inject.unclassed' to
'/usr/local/maldetect/quarantine/gzbase64.inject.unclassed.2818915906'
```

Je relance un scan pour vérifier.
C'est réglé, ça va

```
HOST:      gally
SCAN ID:   160315-1041.2215
STARTED:   mars 15 2016 10:41:18 +0100
COMPLETED: mars 15 2016 10:45:24 +0100
ELAPSED:   246s [find: 0s]

PATH:          /home
TOTAL FILES:   140070
TOTAL HITS:    0
TOTAL CLEANED: 0

=============================================
Linux Malware Detect v1.5 < proj@rfxn.com >
```

suricata

Suricata permet de surveiller les connexions réseaux sur de nombreux services, il joue le role de sentinelle à l'image des suricates d'Afrique.
Suricate va utiliser les captures réalisé avec Pcap, et appliqué des règles définies dans ses fichiers de configuration, il est capable de surveiller de nombreux protocole et adresses
et va exporter les messages dans ses logs.

Le fichiers principal : suricata.yaml ou suricata-debian.yaml (dans mon cas) contient tout l'ensemble de la configuration, address d'ecoute, port, méthode, fichiers de log, contient également la liste
des définitions qui renvoie vers le répertoire /etc/suricata/rules/.
Ce répertoire contient lui même un ensemble de fichiers (aux moins 5 par défault), contenant des templates de motifs à surveiller qu'il faudra activer, en décommentant, et éventuellement adapter en fonction de ses propres besoins.

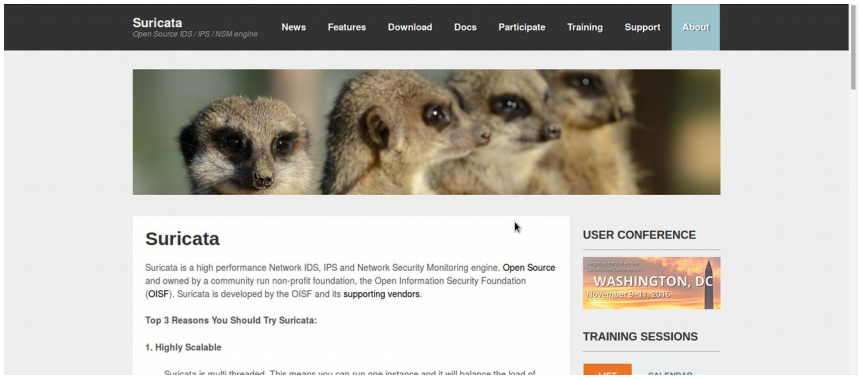
Plus vous parcourrez les fichiers de règles plus vous découvrirez le potentiel du produit.

Attention Suricata n'est pas un Firewall mais fonctionne de paire avec si nécessaire, rappelons qu'ici le but c'est la surveillance, la détection et l'alerte, bien que l'on puisse dropper des packets.

Suricata exporte également ses logs au format json (format riche) qui peut être envoyévers une base de données, à l'aide d'un script python.

Suivant la distribution; la méthode d'installation peut varier, suricata est présente dans mes dépots (mais c'est vrai que j'ai un fichier source un peu personnalisé.)

http://suricata-ids.org/



Download page :http://suricata-ids.org/download/

Installation

Installation depuis les sources

Il faut veiller à la présence du répertoire /var/log/suricata

```
sudo mkdir /var/log/suricata
```

The next step is to copy classification.config, reference.config and suricata.yaml from the base build/installation directory (ex. from git it will be the oisf directory) to the /etc/suricata directory. Do so by entering the following:

```
sudo cp classification.config /etc/suricata
sudo cp reference.config /etc/suricata
sudo cp suricata.yaml /etc/suricata
```

Auto-setup

ex:

```
./configure && make && make install-conf
```

The make install-conf option will do the regular "make install" and then automatically create/setup all the necessary directories and suricata.yaml.

```
./configure && make && make install-rules
```

The make install-rules option will do the regular "make install" and it automatically downloads and sets up the latest ruleset from Emerging Threats available for Suricata.

```
./configure && make && make install-full
```

The make install-full option combines everything mentioned above (install-conf and install-rules) - and will present you with a ready to run (configured and set up) Suricata Setting variables

```
Make sure every variable of the vars, address-groups and port-groups in the yaml file is set
correctly for your needs.

A full explanation is available in the Rule vars section of the yaml. You need to set the ip-
address(es) of your local network
at HOME_NET. It is recommended to set EXTERNAL_NET to !$HOME_NET.
This way, every ip-address but the one set at HOME_NET will be treated as external.

It is also possible to set EXTERNAL_NET to 'any', only the recommended setting is more precise
and lowers the chance that false positives will be generated.
HTTP_SERVERS, SMTP_SERVERS, SQL_SERVERS, DNS_SERVERS and TELNET_SERVERS are by default set to
HOME_NET.
AIM_SERVERS is by default set at 'any'. These variables have to be set for servers on your
network.
All settings have to be set to let it have a more accurate effect.
```

Configuration

Je fournis plus loin les fichiers de règles : yaml rules.
L'équipe de suricata à opté pour ce type de fichier de configuration il est vraiment grand, avec de nombreuses sections. Il n'y a pas de mistères, la configuration du fichier se fera par tatonnement,
suivant l'expérience.

On arrive rarement à une configuration sans messages d'alertes du premier coup.

Le configuration se fera par test successif, et on prendra soin de corriger au fur et à mesure de la progression.

Executer tester

Lancez suricata avec cette commande, regardez les messages d'erreur, et corrigez en fonction.

```
suricata -c /etc/suricata/suricata.yaml -i wlan0 (or eth0)
```

```
suricata -c /etc/suricata/suricata.yaml -i wlan0 (or eth0)

root@gally:/etc/suricata# suricata -c /etc/suricata/suricata-debian.yaml -i wlan0
319/2/2016 -- 17:26:07 - <Notice> - This is Suricata version 2.0.7 RELEASE
419/2/2016 -- 17:26:07 - <Error> - [ERRCODE: SC_ERR_OPENING_RULE_FILE(41)] - opening
rule file /etc/suricata/rules/emerging-icmp.rules: No such file or directory.
519/2/2016 -- 17:26:07 - <Error> - [ERRCODE: SC_ERR_OPENING_RULE_FILE(41)] - opening
rule file /etc/suricata/rules/emerging-imap.rules: No such file or directory.
```

Le message est assez clair : il me manque des fichiers de « rules ».

Corriger

Regles absentes

Suricata ne peut pas ouvrir les fichiers de règles icmp et imap.
Je vais donc récupérer les fichiers manquant, ou je commente la ligne au choix

Les fichiers sont disponibles sur le site emergingthreats.net

```
# wget http://rules.emergingthreats.net/open/suricata/rules/emerging-icmp.rules
--2016-02-19 17:56:51--  http://rules.emergingthreats.net/open/suricata/rules/emerging-icmp.rules
Résolution de rules.emergingthreats.net (rules.emergingthreats.net)… 204.12.217.19, 96.43.137.99
Connexion à rules.emergingthreats.net (rules.emergingthreats.net)|204.12.217.19|:80… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 8657 (8,5K)
Sauvegarde en : « emerging-icmp.rules »
emerging-icmp.rules                 100%
[=====================================================================>]   8,45K
--.-KB/s   ds 0,002s

2016-02-19 17:56:52 (3,45 MB/s) — « emerging-icmp.rules » sauvegardé [8657/8657]
```

Problème de droits

```
19/2/2016 -- 17:08:48 - <Error> - [ERRCODE: SC_ERR_FOPEN(44)] - Error opening file: "/var/log/suricata//fast.log": Permission denied
19/2/2016 -- 17:08:48 - <Error> - [ERRCODE: SC_ERR_FOPEN(44)] - Error opening file: "/var/log/suricata//eve.json": Permission denied
319/2/2016 -- 17:08:48 - <Error> - [ERRCODE: SC_ERR_FOPEN(44)] - failed to open /var/log/suricata//unified2.alert.1455898128: Permission denied
19/2/2016 -- 17:08:48 - <Error> - [ERRCODE: SC_ERR_FOPEN(44)] - Error opening file: "/var/log/suricata//http.log": Permission denied
19/2/2016 -- 17:08:48 - <Warning> - [ERRCODE: SC_ERR_PCAP_CREATE(21)] - Using Pcap capture with GRO or LRO activated can lead to capture problems.
19/2/2016 -- 17:08:48 - <Error> - [ERRCODE: SC_ERR_OPENING_FILE(40)] - Cannot create socket directory /var/run/suricata/: Permission denied
19/2/2016 -- 17:08:48 - <Error> - [ERRCODE: SC_ERR_INITIALIZATION(45)] - Unable to create unix command socket
19/2/2016 -- 17:08:48 - <Notice> - all 7 packet processing threads, 3 management threads initialized, engine started.
^C19/2/2016 -- 17:09:35 - <Notice> - Signal Received.  Stopping engine.
19/2/2016 -- 17:09:35 - <Notice> - Stats for 'wlan0':  pkts: 10, drop: 0 (0.00%), invalid chksum: 0
```

Veillez à créer le répertoire /var/run/suricata

```
mkdir -p /var/log/suricata
chown -R root:suri /var/log/suricata
chmod -R 775 /var/log/suricata
```

PCAP

Oui à l'installation j'avais eu un message prévenant que je n'avais pas le support de pcap.

```
suricata -c /etc/suricata/suricata-debian.yaml -i wlan0
19/2/2016 -- 19:38:19 - <Notice> - This is Suricata version 2.0.7 RELEASE
19/2/2016 -- 19:38:23 - <Warning> - [ERRCODE: SC_ERR_PCAP_CREATE(21)] - Using Pcap
capture with GRO or LRO activated can lead to capture problems.
19/2/2016 -- 19:38:23 - <Notice> - all 22 packet processing threads, 3 management
threads initialized, engine started.
```

Mais si je le laisse tourner et que je le stoppe.
Il voit bien les packets, ce que nous constateront également dans les logs.

```
19/2/2016 -- 18:46:32 - <Warning> - [ERRCODE: SC_ERR_PCAP_CREATE(21)] - Using Pcap
capture with GRO or LRO activated can lead to capture problems.
19/2/2016 -- 18:46:32 - <Notice> - all 22 packet processing threads, 3 management
threads initialized, engine started.
^C19/2/2016 -- 18:50:36 - <Notice> - Signal Received.  Stopping engine.
19/2/2016 -- 18:50:37 - <Notice> - Stats for 'wlan0':  pkts: 1216, drop: 0 (0.00%),
invalid chksum: 0
```

Configuration YAML

Les règles de configurations sont contenu dans le fichier suricata-debian.yaml. Il semble que le yaml soit une syntaxe relativement apprécié , et nous commençons à le trouvé assez souvent, plus d'informations sur le site: yaml.org

Ce fichier de configuration est très grand et contient beaucoup de variables de configuration.

Les identifiants

Par défaut le couple est suri/suri.
Adaptez en fonction de votre système.

```
# Run suricata as user and group.
run-as:
  user: suri
  group: suri
```

Le pid

Créez le fichier de pid.

```
# Default pid file.
# Will use this file if no --pidfile in command options.
pid-file: /var/run/suricata.pid
```

la configuration des interfaces, lan et DMZ.

Attention a vous de définir vos plages, ceci n'est pas configuration.

```
%YAML 1.1
---

# Enable defrag per host settings
#  host-config:
#
#     - dmz:
#         timeout: 30
#         address: [192.168.1.0/24, 127.0.0.0/8, 1.1.1.0/24, 2.2.2.0/24, "1.1.1.1",
"2.2.2.2", "::1"]
#
#     - lan:
#         timeout: 45
#         address:
#           - 192.168.0.0/24
#           - 192.168.10.0/24
#           - 172.16.14.0/24
```

La définitions des fichiers de régles

C'est ici que l'on veille à activer les regles, les regles sont contenu dans des fichiers rangé dans le répertoire rules/.
Vous aurez de nombreux messages vous disant que les fichiers sont manquants.

La règle n'est pas forcément présente, ni configuré.
en l'état ce fichier vous donnera énormément d'erreur de configuration car seule les 6 derniers fichiers existent.
L'équipe de Suricata n'a pas vocation de vous dire quoi surveiller sur vos réseaux et systèmes d'information.

```
# Set the default rule path here to search for the files.
# if not set, it will look at the current working dir
default-rule-path: /etc/suricata/rules
rule-files:
 - botcc.rules
 - ciarmy.rules
 - compromised.rules
 - drop.rules
 - dshield.rules
 - emerging-activex.rules
 - emerging-attack_response.rules
 - emerging-chat.rules
 - emerging-current_events.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-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
 - tor.rules
 - decoder-events.rules # available in suricata sources under rules dir
 - stream-events.rules  # available in suricata sources under rules dir
 - http-events.rules    # available in suricata sources under rules dir
 - smtp-events.rules    # available in suricata sources under rules dir
 - dns-events.rules     # available in suricata sources under rules dir
 - tls-events.rules     # available in suricata sources under rules dir
```

Definition des fichiers de configuration :

classification, et réference

```
classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
```

Variables

adresses et port.

```
# Holds variables that would be used by the engine.
vars:

  # Holds the address group vars that would be passed in a Signature.
  # These would be retrieved during the Signature address parsing stage.
  address-groups:

       HOME_NET: "[192.168.8.0/24]"

      EXTERNAL_NET: "!$HOME_NET"

      HTTP_SERVERS: "$HOME_NET"

      SMTP_SERVERS: "$HOME_NET"

      SQL_SERVERS: "$HOME_NET"

      DNS_SERVERS: "$HOME_NET"

      TELNET_SERVERS: "$HOME_NET"

      AIM_SERVERS: "$EXTERNAL_NET"

      DNP3_SERVER: "$HOME_NET"

      DNP3_CLIENT: "$HOME_NET"
```

```
      MODBUS_CLIENT: "$HOME_NET"

      MODBUS_SERVER: "$HOME_NET"

      ENIP_CLIENT: "$HOME_NET"

      ENIP_SERVER: "$HOME_NET"

  # Holds the port group vars that would be passed in a Signature.
  # These would be retrieved during the Signature port parsing stage.
  port-groups:

      HTTP_PORTS: "80"

      SHELLCODE_PORTS: "!80"

      ORACLE_PORTS: 1521

      SSH_PORTS: 22

      DNP3_PORTS: 20000

# Set the order of alerts bassed on actions
# The default order is pass, drop, reject, alert
action-order:
  - pass
  - drop
  - reject
  - alert
```

IP reputation

Configuration très délicate

Se rentre sur la page de [IP réputation.]

```
# IP Reputation
#reputation-categories-file: /etc/suricata/iprep/categories.txt
#default-reputation-path: /etc/suricata/iprep
#reputation-files:
# - reputation.list
```

```
# Host specific policies for defragmentation and TCP stream
# reassembly.  The host OS lookup is done using a radix tree, just
# like a routing table so the most specific entry matches.
host-os-policy:
  # Make the default policy windows.
  windows: [0.0.0.0/0]
  bsd: []
  bsd-right: []
  old-linux: []
  linux: [10.0.0.0/8, 192.168.1.100, "8762:2352:6241:7245:E000:0000:0000:0000"]
  old-solaris: []
  solaris: ["::1"]
  hpux10: []
  hpux11: []
  irix: []
  macos: []
  vista: []
  windows2k3: []
```

LOG

Activez et définissez vos propres log, et corrigez en fonction des erreurs retournées.

```
# a line based log of HTTP requests (no alerts)
  - http-log:
        enabled: yes
        filename: http.log
        append: yes
        #extended: yes     # enable this for extended logging information
        #custom: yes       # enabled the custom logging format (defined by
customformat)
        #customformat: "%{%D-%H:%M:%S}t.%z %{X-Forwarded-For}i %H %m %h %u %s %B %a:%p
-> %A:%P"
        #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'

  # a line based log of DNS requests and/or replies (no alerts)
  - dns-log:
       enabled: yes
       filename: dns.log
       append: yes
  #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'
            # a line based log to used with pcap file study.
  # this module is dedicated to offline pcap parsing (empty output
  # if used with another kind of input). It can interoperate with
  # pcap parser like wireshark via the suriwire plugin.
  - pcap-info:
       enabled: yes
```

LOG suricata

voir les stats des logs en temps réelle

```
tail -f files-json.log dns.log eve.json fast.log
```

Log eve.json

```
==> eve.json <==
2{"timestamp":"2016-02-
23T00:19:25.851600","event_type":"fileinfo","src_ip":"23.3.235.31","src_port":80,"dest_i
p":"192.168.8.100","dest_port":35992,"proto":"TCP","http":{"url":"\/fwlink\/?
LinkId=275850","hostname":"go.microsoft.com","http_user_agent":"Mozilla\/5.0 (Windows NT
6.3; Win64; x64; Trident\/7.0; rv:11.0) like Gecko\/20100101 Firefox\/12.0"},"fileinfo":
{"filename":"\/fwlink\/","state":"CLOSED","md5":"6e22f0c58e76047aa9a5caad1029a78a","stor
ed":false,"size":190}}
3{"timestamp":"2016-02-
23T00:19:25.862708","event_type":"fileinfo","src_ip":"93.184.220.20","src_port":80,"dest
_ip":"192.168.8.100","dest_port":56071,"proto":"TCP","http":
{"url":"\/CRL\/Omniroot2025.crl","hostname":"cdp1.public-
trust.com","http_user_agent":"Microsoft-CryptoAPI\/6.3"},"fileinfo":
{"filename":"\/CRL\/Omniroot2025.crl","state":"CLOSED","md5":"578cdf52d5a1b67bfeeb7d9931
e8c7b1","stored":false,"size":1830}}
4{"timestamp":"2016-02-
23T00:19:25.862694","event_type":"fileinfo","src_ip":"198.41.215.182","src_port":80,"des
t_ip":"192.168.8.100","dest_port":43264,"proto":"TCP","http":
{"url":"\/MFQwUjBQME4wTDAJBgUrDgMCGgUABBQmECJms4f7i5EbxtN7NbzQCBwAdAQUUa8kJpz0aCJXgCYrO0
ZiFXsezKUCE1oAACvwIEblvrywfQwAAQAAK\/A=","hostname":
```

Suite


```
"ocsp.msocsp.com","http_user_agent":"Microsoft-CryptoAPI\/6.3"},"fileinfo":
{"filename":"\/MFQwUjBQME4wTDAJBgUrDgMCGgUABBQmECJms4f7i5EbxtN7NbzQCBwAdAQUUa8kJpz0aCJXg
CYrO0ZiFXsezKUCE1oAACvwIEblvrywfQwAAQAAK\/A=","state":"CLOSED","md5":"fd81cd29efbf09f1d6
0cb55d2300727f","stored":false,"size":1757}}
5{"timestamp":"2016-02-
23T00:19:25.862626","event_type":"fileinfo","src_ip":"157.56.148.23","src_port":80,"dest
_ip":"192.168.8.100","dest_port":45814,"proto":"TCP","http":{"url":"\/library\/2194da26-
7e64-4497-b4ee-
c2d815f655c0","hostname":"technet.microsoft.com","http_user_agent":"Mozilla\/5.0
(Windows NT 6.3; Win64; x64; Trident\/7.0; rv:11.0) like Gecko\/20100101
Firefox\/12.0"},"fileinfo":{"filename":"\/library\/2194da26-7e64-4497-b4ee-
c2d815f655c0","state":"CLOSED","md5":"4cff6edb9f3730639897479964 9681a3","stored":false,"
size":191}}
6{"timestamp":"2016-02-
23T00:19:18.377094","event_type":"http","src_ip":"192.168.8.100","src_port":45814,"dest_
ip":"157.56.148.23","dest_port":80,"proto":"TCP","http":
{"hostname":"technet.microsoft.com","url":"\/library\/2194da26-7e64-4497-b4ee-
c2d815f655c0","http_user_agent":"Mozilla\/5.0 (Windows NT 6.3; Win64; x64; Trident\/7.0;
rv:11.0) like Gecko\/20100101 Firefox\/12.0","accept_encoding":"gzip,
deflate","accept_language":"fr-
FR","http_method":"GET","protocol":"HTTP\/1.1","status":"301","redirect":"https:\/\/tech
net.microsoft.com\/library\/2194da26-7e64-4497-b4ee-c2d815f655c0","length":191}}
7{"timestamp":"2016-02-
23T00:19:22.945821","event_type":"tls","src_ip":"192.168.8.100","src_port":43421,"dest_i
p":"157.56.148.23","dest_port":443,"proto":"TCP","tls":
{"subject":"CN=technet.microsoft.com","issuerdn":"C=US, ST=Washington, L=Redmond,
O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft IT SSL
SHA2","fingerprint":"bd:2a:b0:61:6e:16:28:2b:86:8d:71:06:16:c7:c8:5a:52:af:11:ac","versi
on":"TLS 1.2"}}
8{"timestamp":"2016-02-
23T00:19:23.188761","event_type":"http","src_ip":"192.168.8.100","src_port":48449,"dest_
ip":"90.84.59.88","dest_port":80,"proto":"TCP","http":
{"hostname":"ctldl.windowsupdate.com","url":"\/msdownload\/update\/v3\/static\/trustedr\
/en\/authrootstl.cab?52c7fb89109fc4b8","http_user_agent":"Microsoft-
CryptoAPI\/6.3","http_content_type":"application\/octet-
stream","http_method":"GET","protocol":"HTTP\/1.1","status":"200","length":49661}}
```

Log files-json

```
==> files-json.log <==
11{ "timestamp": "02\/23\/2016-00:19:25.851600", "ipver": 4, "srcip": "23.3.235.31",
"dstip": "192.168.8.100", "protocol": 6, "sp": 80, "dp": 35992, "http_uri": "\/fwlink\/?
LinkId=275850", "http_host": "go.microsoft.com", "http_referer": "<unknown>",
"http_user_agent": "Mozilla\/5.0 (Windows NT 6.3; Win64; x64; Trident\/7.0; rv:11.0)
like Gecko\/20100101 Firefox\/12.0", "filename": "\/fwlink\/", "magic": "unknown",
"state": "CLOSED", "md5": "6e22f0c58e76047aa9a5caad1029a78a", "stored": false, "size":
190 }
12{ "timestamp": "02\/23\/2016-00:19:25.862708", "ipver": 4, "srcip": "93.184.220.20",
"dstip": "192.168.8.100", "protocol": 6, "sp": 80, "dp": 56071, "http_uri":
"\/CRL\/Omniroot2025.crl", "http_host": "cdp1.public-trust.com", "http_referer":
"<unknown>", "http_user_agent": "Microsoft-CryptoAPI\/6.3", "filename":
"\/CRL\/Omniroot2025.crl", "magic": "unknown", "state": "CLOSED", "md5":
"578cdf52d5a1b67bfeeb7d9931e8c7b1", "stored": false, "size": 1830 }
13{ "timestamp": "02\/23\/2016-00:19:25.862694", "ipver": 4, "srcip": "198.41.215.182",
"dstip": "192.168.8.100", "protocol": 6, "sp": 80, "dp": 43264, "http_uri":
"\/MFQwUjBQME4wTDAJBgUrDgMCGgUABBQmECJms4f7i5EbxtN7NbzQCBwAdAQUUa8kJpz0aCJXgCYrO0ZiFXsez
KUCE1oAACvwIEblvrywfQwAAQAAK\/A=", "http_host": "ocsp.msocsp.com", "http_referer":
"<unknown>", "http_user_agent": "Microsoft-CryptoAPI\/6.3", "filename":
"\/MFQwUjBQME4wTDAJBgUrDgMCGgUABBQmECJms4f7i5EbxtN7NbzQCBwAdAQUUa8kJpz0aCJXgCYrO0ZiFXsez
KUCE1oAACvwIEblvrywfQwAAQAAK\/A=", "magic": "unknown", "state": "CLOSED", "md5":
"fd81cd29efbf09f1d60cb55d2300727f", "stored": false, "size": 1757 }
14{ "timestamp": "02\/23\/2016-00:19:25.862626", "ipver": 4, "srcip": "157.56.148.23",
"dstip": "192.168.8.100", "protocol": 6, "sp": 80, "dp": 45814, "http_uri":
"\/library\/2194da26-7e64-4497-b4ee-c2d815f655c0", "http_host": "technet.microsoft.com",
"http_referer": "<unknown>", "http_user_agent": "Mozilla\/5.0 (Windows NT 6.3; Win64;
x64; Trident\/7.0; rv:11.0) like Gecko\/20100101 Firefox\/12.0", "filename":
"\/library\/2194da26-7e64-4497-b4ee-c2d815f655c0", "magic": "unknown", "state":
"CLOSED", "md5": "4cff6edb9f37306398974799649681a3", "stored": false, "size": 191 }
15{ "timestamp": "02\/23\/2016-00:19:25.862722", "ipver": 4, "srcip": "90.84.59.88",
"dstip": "192.168.8.100", "protocol": 6, "sp": 80, "dp": 48449, "http_uri":
"\/msdownload\/update\/v3\/static\/trustedr\/en\/authrootstl.cab?52c7fb89109fc4b8",
"http_host": "ctldl.windowsupdate.com", "http_referer": "<unknown>", "http_user_agent":
"Microsoft-CryptoAPI\/6.3", "filename":
"\/msdownload\/update\/v3\/static\/trustedr\/en\/authrootstl.cab", "magic": "unknown",
"state": "CLOSED", "md5": "d0baf8cf78a8d6fe0d05615f3c8b708a", "stored": false, "size":
3589 }
```

Log http-log

```
tail -f http.log stats.log
detect.alert                | Detect                    | 0
flow_mgr.closed_pruned      | FlowManagerThread         | 16
flow_mgr.new_pruned         | FlowManagerThread         | 15
flow_mgr.est_pruned         | FlowManagerThread         | 16
flow.memuse                 | FlowManagerThread         | 7077472
flow.spare                  | FlowManagerThread         | 10000
flow.emerg_mode_entered     | FlowManagerThread         | 0
flow.emerg_mode_over        | FlowManagerThread         | 0
-------------------------------------------------------------------
Date: 2/22/2016 -- 19:59:23 (uptime: 0d, 00h 03m 15s)
-------------------------------------------------------------------
Counter                     | TM Name                   | Value
-------------------------------------------------------------------
dns.memuse                  | Recv-Q0                   | 0
dns.memcap_state            | Recv-Q0                   | 0
dns.memcap_global           | Recv-Q0                   | 0
decoder.pkts                | Recv-Q0                   | 0
decoder.bytes               | Recv-Q0                   | 0
decoder.invalid             | Recv-Q0                   | 0
```

http log

Surligné en jaune dans cette section.

```
02/19/2016-17:50:15.061973 rules.emergingthreats.net [**] /open/suricata/rules/emerging-
worm.rules [**] Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0
Iceweasel/38.5.0 [**] 192.168.8.100:48540 -> 204.12.217.19:80
02/19/2016-17:51:17.425335 rules.emergingthreats.net [**] /open/suricata/rules/emerging-
icmp.rules [**] Wget/1.16 (linux-gnu) [**] 192.168.8.100:48545 -> 204.12.217.19:80
02/19/2016-17:56:25.623172 rules.emergingthreats.net [**] /open/suricata/rules/emerging-
inappropriate.rules [**] Wget/1.16 (linux-gnu) [**] 192.168.8.100:48552 ->
204.12.217.19:80
02/19/2016-17:56:52.480431 rules.emergingthreats.net [**] /open/suricata/rules/emerging-
icmp.rules [**] Wget/1.16 (linux-gnu) [**] 192.168.8.100:48553 -> 204.12.217.19:80


root@gally:/var/log/suricata#

02/20/2016-07:22:29.184403 1.1.1.3 [**] /bmi/www.malware-traffic-
analysis.net/2016/02/06/2016-02-06-traffic-analysis-exercise-image-01.jpg [**]
Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.5.0
[**] 192.168.8.100:52898 -> 1.1.1.3:80
02/20/2016-07:22:29.185090 1.1.1.4 [**] /bmi/www.malware-traffic-
analysis.net/2016/02/06/2016-02-06-traffic-analysis-exercise-image-02.jpg [**]
Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.5.0
[**] 192.168.8.100:53027 -> 1.1.1.4:80
02/20/2016-07:22:30.178623 www.malware-traffic-analysis.net [**] /2016/02/06/2016-02-06-
traffic-analysis-exercise-image-02.jpg [**] Mozilla/5.0 (X11; Linux x86_64; rv:38.0)
Gecko/20100101 Firefox/38.0 Iceweasel/38.5.0 [**] 192.168.8.100:49849 ->
166.78.135.34:80
```

Fast log

Attention au niveau d'alerte, ici mal configuré suricata est tout excité, et c'est moi qui faisais des wget sur l'adresse du site partenaire de suricata qui héberge les fichier de régles.

```
-[/var/log/suricata]-[21:15]-->
>~ cat fast.log
02/22/2016-21:06:13.431251  [**] [1:2200029:1] SURICATA ICMPv6 unknown type [**]
[Classification: (null)] [Priority: 3] {IPv6-ICMP}
0000:0000:0000:0000:0000:0000:0000:0143 -> ff02:0000:0000:0000:0000:0000:0000:0016:0
02/22/2016-21:06:13.431251  [**] [1:2200094:1] SURICATA zero length padN option [**]
[Classification: (null)] [Priority: 3] {IPv6-ICMP}
0000:0000:0000:0000:0000:0000:0000:0143 -> ff02:0000:0000:0000:0000:0000:0000:0016:0
```

Encore un petit effort...

```
02/20/2016-07:27:09.431846  [**] [1:2210010:2] SURICATA STREAM 3way handshake wrong seq
wrong ack [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP}
192.168.8.100:32993 -> 3.235.43.133:443
```

EVE log


```
{"timestamp":"2016-02-
22T20:56:53.659874","event_type":"dns","src_ip":"192.168.8.100","src_port":21595,"dest_i
p":"80.67.169.12","dest_port":53,"proto":"UDP","dns":
{"type":"query","id":21406,"rrname":"cUrrENT.Cvd.clamAV.neT","rrtype":"TXT"}}
{"timestamp":"2016-02-
22T20:56:53.659874","event_type":"dns","src_ip":"80.67.169.12","src_port":53,"dest_ip":"
192.168.8.100","dest_port":21595,"proto":"UDP","dns":
{"type":"answer","id":21406,"rrname":"cUrrENT.Cvd.clamAV.neT","rrtype":"TXT","ttl":56,"r
data":"0.99:55:21400:1456165740:1:63:44434:271"}}
{"timestamp":"2016-02-
22T20:56:53.659874","event_type":"dns","src_ip":"80.67.169.12","src_port":53,"dest_ip":"
192.168.8.100","dest_port":21595,"proto":"UDP","dns":
{"type":"answer","id":21406,"rrname":"Cvd.clamAV.neT","rrtype":"NS","ttl":5456}}
```


DNS log

Parfait, je constate que unbound est bien réglé, il me fait la récursivité.

```
-[/var/log/suricata]-[21:16]-->
>~ cat dns.log
02/22/2016-20:56:53.659874 [**] Query TX 539e [**] cUrrENT.Cvd.clamAV.neT [**] TXT [**]
192.168.8.100:21595 -> 80.67.169.12:53
02/22/2016-20:56:53.659874 [**] Response TX 539e [**] Recursion Desired [**]
80.67.169.12:53 -> 192.168.8.100:21595
02/22/2016-20:56:53.659874 [**] Response TX 539e [**] cUrrENT.Cvd.clamAV.neT [**] TXT
[**] TTL 56 [**] 0.99:55:21400:1456165740:1:63:44434:271 [**] 80.67.169.12:53 ->
192.168.8.100:21595
02/22/2016-20:56:53.659874 [**] Response TX 539e [**] Cvd.clamAV.neT [**] NS [**] TTL
5456 [**] ns5.clamAV.neT [**] 80.67.169.12:53 -> 192.168.8.100:21595
02/22/2016-20:56:53.659874 [**] Response TX 539e [**] Cvd.clamAV.neT [**] NS [**] TTL
5456 [**] ns4.clamAV.neT [**] 80.67.169.12:53 -> 192.168.8.100:21595
02/22/2016-20:56:53.659874 [**] Response TX 539e [**] Cvd.clamAV.neT [**] NS [**] TTL
5456 [**] ns6.clamAV.neT [**] 80.67.169.12:53 -> 192.168.8.100:21595
02/22/2016-20:56:53.659874 [**] Response TX 539e [**] Cvd.clamAV.neT [**] NS [**] TTL
5456 [**] ns7.clamAV.neT [**] 80.67.169.12:53 -> 192.168.8.100:21595
02/22/2016-20:56:53.659874 [**] Response TX 539e [**] Cvd.clamAV.neT [**] NS [**] TTL
5456 [**] ns3.clamAV.neT [**] 80.67.169.12:53 -> 192.168.8.100:21595
```

rules

Voici pour l'instant la liste, que j'ai constitué.

```
# Set the default rule path here to search for the files.
# if not set, it will look at the current working dir
default-rule-path: /etc/suricata/rules
rule-files:
                # - botcc.rules
                # - ciarmy.rules
                # - compromised.rules
                # - drop.rules
                # - dshield.rules
                # - emerging-activex.rules
                # - emerging-attack_response.rules
                # - emerging-chat.rules
                # - emerging-current_events.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-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
   # - tor.rules
 - decoder-events.rules # available in suricata sources under rules dir
 - stream-events.rules  # available in suricata sources under rules dir
 - http-events.rules    # available in suricata sources under rules dir
 - smtp-events.rules    # available in suricata sources under rules dir
 - dns-events.rules     # available in suricata sources under rules dir
 - tls-events.rules     # available in suricata sources under rules dir
```

Jettons un oeil à inappropiate.rules.

Inapropriate

Voici 3 lignes du fichiers, celui-ci se concentre sur le contenu de la requête, c'est très explicite...
Vous l'avez compris il s'agit du porno.

```
#
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL INAPPROPRIATE fuck movies";
flow:to_client,established; content:"fuck movies"; nocase; classtype:policy-violation;
sid:2101320; rev:9;)
#
#
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL INAPPROPRIATE hardcore anal";
flow:to_client,established; content:"hardcore anal"; nocase; classtype:policy-violation;
sid:2101311; rev:9;)
#
#


alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL INAPPROPRIATE hardcore rape";
flow:to_client,established; content:"hardcore rape"; nocase; classtype:policy-violation;
sid:2101318; rev:9;)
```

Ou de voir si le mode safe est activé ou non pour google image.

```
# This Ruleset is EmergingThreats Open optimized for suricata.
#Google Image Search, Safe Mode Off
#
alert http $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET INAPPROPRIATE Google
Image Search, Safe Mode Off"; flow:established,to_server; uricontent:"&safe=off";
content:"|0d 0a|Host|3a| images.google.com|0d 0a|";
reference:url,doc.emergingthreats.net/bin/view/Main/2002925; classtype:policy-violation;
sid:2002925; rev:5;)
```

Netbios

Celui-ci vise particulièrement les attaques sur le Netbios

```
# This Ruleset is EmergingThreats Open optimized for suricata.
#by Christopher Campesi
#
#alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS Remote SMB2.0 DoS
Exploit"; flow:to_server,established; content:"|ff|SMB|72 00 00 00 00 18 53 c8|";
offset:4; content:!"|00 00|"; within:2;
reference:url,securityreason.com/exploitalert/7138;
reference:url,doc.emergingthreats.net/2009886; classtype:attempted-dos; sid:2009886;
rev:4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS MS04011 Lsasrv.dll RPC
exploit (Win2k)"; flow: to_server,established; content:"|00 00 00 00 9A A8 40 00 01 00
00 00 00 00 00 00|"; content:"|01 0000 00 00 00 00 00 9A A8 40 00 01 00 00 00|";
reference:url,doc.emergingthreats.net/bin/view/Main/2000046; reference:cve,2003-0533;
classtype:misc-activity; sid:2000046; rev:9;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS MS04011 Lsasrv.dll RPC
exploit (WinXP)"; flow: to_server,established; content:"|95 14 40 00 03 00 00 00 7C 70
40 00 01|"; content:"|78 85 13 00 AB5B A6 E9 31 31|";
reference:url,doc.emergingthreats.net/bin/view/Main/2000033; reference:cve,2003-0533;
classtype:misc-activity; sid:2000033; rev:9;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"ET NETBIOS MS04-007 Kill-Bill ASN1
exploit attempt"; flow: established,to_server; content:"CCCC|20f0fd7f|SVWf";
reference:url,www.phreedom.org/solar/exploits/msasn1-bitstring/;
reference:url,www.microsoft.com/technet/security/bulletin/MS04-007.mspx;
reference:cve,CAN-2003-0818;
reference:url,doc.emergingthreats.net/bin/view/Main/2001944; classtype:attempted-admin;
sid:2001944; rev:7;)
```

Web-server

La surveillance du site web se configure ici.

```
# This Ruleset is EmergingThreats Open optimized for suricata.

#by mike cox
#
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET WEB_SERVER RFI Scanner Success
(Fx29ID)"; flow:established,from_server; content:"FeeLCoMzFeeLCoMz";
reference:url,doc.emergingthreats.net/2010463;
reference:url,opinion.josepino.com/php/howto_website_hack1; classtype:successful-user;
sid:2010463; rev:7;)

#
#alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WEB_SERVER Possible File
Injection Compromise (HaCKeD By BeLa & BodyguarD)"; flow:established,to_server;
content:"HaCKeD By BeLa & BodyguarD"; reference:url,www.incidents.org/diary.html?
storyid=4405; classtype:web-application-attack; sid:2008207; rev:5;)

#Mark Tombaugh
```

```
#
#alert http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET WEB_SERVER XML-RPC for PHP
Remote Code Injection"; flow:established,to_server; content:"POST"; nocase; http_method;
content:"xmlrpc.php"; http_uri; content:"methodCall"; http_client_body; nocase;
pcre:"/>.*?\'\s*?\)\s*?\)*?\s*?\;/PR";
reference:url,www.securityfocus.com/bid/14088/exploit; reference:cve,2005-1921;
reference:url,doc.emergingthreats.net/bin/view/Main/2002158; classtype:web-application-
attack; sid:2002158; rev:14;)

#by Kevin ross and mike cox
#
alert http $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET WEB_SERVER Possible 3Com
OfficeConnect Router Default User Account Remote Command Execution Attempt";
flow:established,to_server; uricontent:"/utility.cgi?testType="; nocase;
uricontent:"IP="; nocase; uricontent:"|7C 7C|"; pcre:"/\x7C\x7C.+[a-z]/Ui";
reference:url,securitytracker.com/alerts/2009/Oct/1023051.html;
reference:url,www.securityfocus.com/archive/1/507263;
reference:url,www.securityfocus.com/bid/36722/info;
reference:url,doc.emergingthreats.net/2010159; classtype:attempted-admin; sid:2010159;
rev:4;)

#by kevin ross
#
alert http $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SERVER 3Com
Intelligent Management Center Cross Site Scripting Attempt"; flow:established,to_server;
uricontent:"/imc/login.jsf"; nocase; uricontent:"loginForm"; nocase;
uricontent:"javax.faces.ViewState="; nocase; pcre:"/ViewState\x3D.+(script|alert|
onmouse[a-z]+|onkey[a-z]+|onload|onunload|ondragdrop|onblur|onfocus|onclick|ondblclick|
onsubmit|onreset|onselect|onchange)/Ui";
reference:url,securitytracker.com/alerts/2010/May/1024022.html;
reference:url,support.3com.com/documents/netmgr/imc/3Com_IMC_readme_plat_3.30-SP2.html;
reference:url,www.procheckup.com/vulnerability_manager/vulnerabilities/pr10-02;
reference:url,doc.emergingthreats.net/2011145; classtype:web-application-attack;
sid:2011145; rev:3;)

#by kevin ross and evilghost
#
alert http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET WEB_SERVER Apache mod_perl
Apache Status and Apache2 Status Cross Site Scripting Attempt";
flow:established,to_server; content:"|2F|APR|3A 3A|SockAddr|3A 3A|port|2F|"; http_uri;
nocase; pcre:"/(script|img|src|alert|onmouse|onkey|onload|ondragdrop|onblur|onfocus|
onclick)/Ui"; reference:url,www.securityfocus.com/bid/34383/info; reference:cve,2009-
0796; reference:url,doc.emergingthreats.net/2010281; classtype:attempted-user;
sid:2010281; rev:4;)
```

Web-client

Celui est excellent, il surveille les appel d'application, par contre attention si vous surveillez un réseau sur lequel des dévellopeurs vont se connecter à une base de données, ne soyez pas étonnés d'avoir beaucoup d'alertes.

```
# This Ruleset is EmergingThreats Open optimized for suricata.

#by kevin ross
#
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Adobe
Multimedia Doc.media.newPlayer Memory Corruption Attempt"; flow:to_client,established;
content:"PDF-"; depth:300; content:"this.media.newPlayer|28|null"; nocase; distance:0;
content:"util.printd"; nocase; within:150;
reference:url,www.metasploit.com/redmine/projects/framework/repository/revisions/7881/en
try/modules/exploits/windows/fileformat/adobe_media_newplayer.rb; reference:url,vrt-
sourcefire.blogspot.com/2009/12/adobe-reader-medianewplayer-analysis.html;
reference:bid,37331; reference:cve,2009-4324; classtype:attempted-user; sid:2010495;
rev:14;)
```

```
#kevin ross
#
alert http $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Adobe
Reader and Acrobat Forms Data Format Remote Security Bypass Attempt";
flow:established,to_client; content:"|0d 0a|%FDF-"; depth:600; content:"/F(JavaScript|
3a|"; nocase; distance:0; reference:url,www.securityfocus.com/bid/37763;
reference:cve,2009-3956; reference:url,doc.emergingthreats.net/2010664;
reference:url,www.stratsec.net/files/SS-2010-
001_Stratsec_Acrobat_Script_Injection_Security_Advisory_v1.0.pdf; classtype:attempted-
user; sid:2010664; rev:5;)

#by kevin ross
#needs removed somewhere around the end of may 2010
#Modified Slightly to Improve Detection (Action seems to be able to come either side of
Launch so removed it and left in launch and win and added in a content match for .exe
#
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Foxit/Adobe
PDF Reader Launch Action Remote Code Execution Attempt"; flow:to_client,established;
content:"PDF-"; depth:300; content:"Launch"; distance:0; content:"Win"; distance:0;
content:".exe"; nocase; distance:0; reference:url,www.kb.cert.org/vuls/id/570177;
reference:url,www.h-online.com/security/news/item/Criminals-attempt-to-exploit-
unpatched-hole-in-Adobe-Reader-979286.html;
reference:url,www.sudosecure.net/archives/673; reference:url,www.h-
online.com/security/news/item/Adobe-issues-official-workaround-for-PDF-vulnerability-
971932.html; reference:url,blog.didierstevens.com/2010/03/31/escape-from-foxit-reader/;
reference:url,www.m86security.com/labs/i/PDF-Launch-Feature-Used-to-Install-
Zeus,trace.1301~.asp; reference:url,doc.emergingthreats.net/2010968;
classtype:attempted-user; sid:2010968; rev:7;)

#by kevin ross
#A bit more basic detection for the Java Exploit
#
alert http $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Java
Deployment Toolkit Launch Method Remote Code Execution Attempt";
flow:established,to_client; content:"-J-jar -J"; pcre:"/(launch\x28.+-J-jar -J|-J-jar
-J.+launch\x28)/i"; reference:url,seclists.org/fulldisclosure/2010/Apr/119;
reference:url,www.darknet.org.uk/2010/04/serious-java-bug-exposes-users-to-code-
execution/; reference:url,doc.emergingthreats.net/2011053; classtype:attempted-user;
sid:2011053; rev:3;)

#by mike cox
#
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Java Web Start
Command Injection (.jar)"; flow:established,from_server; content:"http|3a| -J-jar -J|5C
5C 5C 5C|"; nocase; content:".launch("; nocase; pcre:"/http\x3a -J-jar
-J\x5C\x5C\x5C\x5C\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\x5C\x5C[^\n]*\.jar/i";
reference:url,seclists.org/fulldisclosure/2010/Apr/119;
reference:url,doc.emergingthreats.net/2011698; classtype:web-application-attack;
sid:2011698; rev:6;)
```

TLS

Surveillance de la validité des certificats.

```
# TLS event  rules
#
# SID's fall in the 2230000+ range. See
http://doc.emergingthreats.net/bin/view/Main/SidAllocation
#
# These sigs fire at most once per connection.
#
# A flowint tls.anomaly.count is incremented for each match. By default it will be 0.
#
```

```
alert tls any any -> any any (msg:"SURICATA TLS invalid SSLv2 header"; flow:established;
app-layer-event:tls.invalid_sslv2_header; flowint:tls.anomaly.count,+,1;
classtype:protocol-command-decode; sid:2230000; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS invalid TLS header"; flow:established;
app-layer-event:tls.invalid_tls_header; flowint:tls.anomaly.count,+,1;
classtype:protocol-command-decode; sid:2230001; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS invalid record version";
flow:established; app-layer-event:tls.invalid_record_version; flowint:tls.anomaly.count,
+,1; classtype:protocol-command-decode; sid:2230015; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS invalid record type"; flow:established;
app-layer-event:tls.invalid_record_type; flowint:tls.anomaly.count,+,1;
classtype:protocol-command-decode; sid:2230002; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS invalid handshake message";
flow:established; app-layer-event:tls.invalid_handshake_message;
flowint:tls.anomaly.count,+,1; classtype:protocol-command-decode; sid:2230003; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS invalid certificate"; flow:established;
app-layer-event:tls.invalid_certificate; flowint:tls.anomaly.count,+,1;
classtype:protocol-command-decode; sid:2230004; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS certificate missing element";
flow:established; app-layer-event:tls.certificate_missing_element;
flowint:tls.anomaly.count,+,1; classtype:protocol-command-decode; sid:2230005; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS certificate unknown element";
flow:established; app-layer-event:tls.certificate_unknown_element;
flowint:tls.anomaly.count,+,1; classtype:protocol-command-decode; sid:2230006; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS certificate invalid length";
flow:established; app-layer-event:tls.certificate_invalid_length;
flowint:tls.anomaly.count,+,1; classtype:protocol-command-decode; sid:2230007; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS certificate invalid string";
flow:established; app-layer-event:tls.certificate_invalid_string;
flowint:tls.anomaly.count,+,1; classtype:protocol-command-decode; sid:2230008; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS error message encountered";
flow:established; app-layer-event:tls.error_message_encountered;
flowint:tls.anomaly.count,+,1; classtype:protocol-command-decode; sid:2230009; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS invalid record/traffic";
flow:established; app-layer-event:tls.invalid_ssl_record; flowint:tls.anomaly.count,+,1;
classtype:protocol-command-decode; sid:2230010; rev:1;)

alert tls any any -> any any (msg:"SURICATA TLS heartbeat encountered";
flow:established; app-layer-event:tls.heartbeat_message; flowint:tls.anomaly.count,+,1;
classtype:protocol-command-decode; sid:2230011; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS overflow heartbeat encountered, possible
exploit attempt (heartbleed)"; flow:established; app-layer-
event:tls.overflow_heartbeat_message; flowint:tls.anomaly.count,+,1; classtype:protocol-
command-decode; reference:cve,2014-0160; sid:2230012; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS invalid heartbeat encountered, possible
exploit attempt (heartbleed)"; flow:established; app-layer-
event:tls.invalid_heartbeat_message; flowint:tls.anomaly.count,+,1; classtype:protocol-
command-decode; reference:cve,2014-0160; sid:2230013; rev:1;)
alert tls any any -> any any (msg:"SURICATA TLS invalid encrypted heartbeat encountered,
possible exploit attempt (heartbleed)"; flow:established; app-layer-
event:tls.dataleak_heartbeat_mismatch; flowint:tls.anomaly.count,+,1;
classtype:protocol-command-decode; reference:cve,2014-0160; sid:2230014; rev:1;)

#next sid is 2230016
```

SQL

Ici également il faut veiller à ce que la configuration corresponde avec votre système.

```
# This Ruleset is EmergingThreats Open optimized for suricata.

#kevin ross
#
#alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 1433 (msg:"ET SQL MSSQL
sp_replwritetovarbin - potential memory overwrite case 1"; flow:to_server,established;
content:"s|00|p|00|_|00|r|00|e|00|p|00|l|00|w|00|r|00|i|00|t|00|e|00|t|00|o|00|v|00|a|
00|r|00|b|00|i|00|n"; nocase;
reference:url,archives.neohapsis.com/archives/fulldisclosure/2008-12/0239.html;
reference:url,doc.emergingthreats.net/bin/view/Main/2008909; classtype:attempted-user;
sid:2008909; rev:2;)

#
alert http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"GPL SQL Oracle iSQLPlus
login.uix username overflow attempt"; flow:to_server,established; content:"/login.uix";
fast_pattern:only; http_uri; nocase; content:"username="; nocase; isdataat:250,relative;
content:!"|0A|"; within:250; pcre:"/username=[^&\x3b\r\n]{250}/smi";
reference:bugtraq,10871; reference:url,www.nextgenss.com/advisories/ora-isqlplus.txt;
classtype:web-application-attack; sid:2102703; rev:5;)

#
#alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS (msg:"GPL SQL EXECUTE_SYSTEM
attempt"; flow:to_server,established; content:"EXECUTE_SYSTEM"; nocase;
classtype:system-call-detect; sid:2101673; rev:4;)

#
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS (msg:"GPL SQL TO_CHAR buffer
overflow attempt"; flow:to_server,established; content:"TO_CHAR"; nocase;
pcre:"/TO_CHAR\s*\(\s*SYSTIMESTAMP\s*,\s*(\x27[^\x27]{256}|\x22[^\x22]{256})/smi";
classtype:attempted-user; sid:2102699; rev:2;)
```

BONUS

Services inutiles

Desactiver les services qui ne servent pas...
Si vous n'utilisez pas les services portmap, nfs et inetd (dans le cas d'un serveur web vous n'en avez pas besoin).
Il en existe d'autres, selon votre distribution et les choix d'installation originaux.
Vous économiserez aussi en mémoire vive.

Attention à ce que vous désactivez

```
/etc/init.d/portmap stop

/etc/init.d/nfs-common stop

update-rc.d -f portmap remove

update-rc.d -f nfs-common remove

update-rc.d -f inetd remove

apt-get remove portmap

apt-get remove ppp
```

Autorisations diverses

N'autorisons les compilateurs et installeurs que pour root (le numéro de version est à adapter selon la fraîcheur de votre installation) :

```
chmod o-x /usr/bin/gcc-4.1
chmod o-x /usr/bin/make
chmod o-x /usr/bin/apt-get
chmod o-x /usr/bin/aptitude
chmod o-x /usr/bin/dpkg
```