Ασφάλεια Δικτύων και Επικοινωνιών

(Network and Communication Security)

OSSEC host-based ids

Αν. Καθ. Παναγιώτης Κοτζανικολάου

Υπ.Διδ. Δημήτρης Κούτρας

ΠΜΣ Κυβερνοασφάλεια και Επιστήμη Δεδομένων

OSSEC

- Open source host-based ids
- Υποστηρίζει:
  - log analysis
  - file integrity checking
  - policy monitoring
  - rootkit detection
  - real-time alerting
  - active response
- http://www.ossec.net/

OSSEC INSTALLATION

sudo –s
apt-get update
apt-get install build-essential inotify-tools
sudo apt-get install apache2 -y
sudo apt-get install build-essential -y
sudo apt-get update -y
wget https://github.com/ossec/ossec-hids/archive/2.9.2.tar.gz
sudo tar -zxvf 2.9.2.tar.gz
cd ossec-hids-2.9.2/
sudo ./install.sh
sudo /var/ossec/bin/ossec-control start
cd /home/ubuntuVM (name of your pc)
wget https://github.com/ossec/ossec-wui/archive/master.zip
sudo apt-get install unzip -y
sudo unzip master.zip
mv ossec-wui-master /var/www/html/ossec
cd /var/www/html/ossec
./setup.sh
systemctl restart apache2
sudo apt-get update -y
sudo apt-get install php -y

sudo apt-get install apache2 php-mysql libapache2-mod-php mysql-server

sudo apt-get update

sudo add-apt-repository ppa:ondrej/php

sudo apt-get update

sudo apt search php7

sudo apt install php7.0-mysql php7.0-curl php7.0-json php7.0-cgi php7.0 libapache2-mod-php7.0

sudo apt-get install build-essential gcc make apache2 libapache2-mod-php7.0 php7.0 php7.0-cli php7.0-common apache2-utils unzip wget sendmail inotify-tools -y

OSSEC

- **Εάν η εγκατάσταση ολοκληρωθεί επιτυχώς θα εμφανιστούν τα παρακάτω μηνύματα:**

- System is Debian (Ubuntu or derivative).
- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:
  /var/OSSEC/bin/OSSEC-control start

- To stop OSSEC HIDS:
  /var/OSSEC/bin/OSSEC-control stop

- The configuration can be viewed or modified at /var/OSSEC/etc/OSSEC.conf

Thanks for using the OSSEC HIDS.
If you have any question, suggestion or if you find any bug,
contact us at contact@OSSEC.net or using our public maillist at
OSSEC-list@OSSEC.net
(http://www.OSSEC.net/main/support/).

More information can be found at http://www.OSSEC.net

--- Press ENTER to finish (maybe more information below). ---

OSSEC

Αυτοματοποιημένες Διαδικασίες Άμυνας

Ύπαρξη ενσωματωμένων και αυτοματοποιημένων διαδικασιών αυτοάμυνας και συντήρησης.

Έλεγχος Ακεραιότητας Συστήματος

- **System Check**
  τακτικός έλεγχος ακεραιότητας του συστήματος
- **Rootkit Check**
  εξασφάλιση της μη προσβολής του συστήματος από rootkits

Άμεση Αναφορά Ύποπτων Ενεργειών

Άμεση ενημέρωση του διαχειριστή για οποιοδήποτε συμβάν με σχετικές πληροφορίες.

OSSEC

Εγκατάσταση Rootcheck

- **Εκτελούμε από terminal:**

```
cd Downloads
wget https://dcid.me/ossec-packages/rootcheck-latest.tar.gz
tar -zxvf rootcheck-latest.tar.gz
cd rootcheck***/
./install.sh
./rootcheck
```

OSSEC

Εκκίνηση και τερματισμός του OSSEC

- **Για να ξεκινήσει το OSSEC τρέχουμε την παρακάτω εντολή στο terminal:**

/var/OSSEC/bin/OSSEC-control start

- **Για να σταματήσουμε το OSSEC τρέχουμε την εντολή:**

/var/OSSEC/bin/OSSEC-control stop

- **Για να επανεκκινήσουμε το OSSEC τρέχουμε την εντολή:**

/var/OSSEC/bin/OSSEC-control restart

- **Για να δούμε την τρέχουσα κατάσταση του OSSEC τρέχουμε την εντολή:**

/var/OSSEC/bin/OSSEC-control status

OSSEC

- **Εάν το OSSEC έχει ξεκινήσει η έξοδος της εντολής θα πρέπει να μοιάζει με την παρακάτω:**

```
OSSEC-monitord is running...
OSSEC-logcollector is running...
OSSEC-syscheckd is running...
OSSEC-analysisd is running...
OSSEC-maild is running...
OSSEC-execd is running...
```

- **Εάν δεν έχει ξεκινήσει η έξοδος θα μοιάζει με την παρακάτω:**

```
OSSEC-monitord not running...
OSSEC-logcollector not running...
OSSEC-syscheckd not running...
OSSEC-analysisd not running...
OSSEC-maild not running...
OSSEC-execd not running...
```

OSSEC

Ossec.conf -> https://github.com/ossec/ossec-hids/blob/master/etc/ossec.conf

Decoders -> https://github.com/ossec/ossec-rules/blob/master/decoders.d/50-crs-apache_decoder.xml

Rules -> https://github.com/ossec/ossec-rules/blob/master/rules.d/50-crs-apache_rules.xml

Το ossec βασίζεται σε κανόνες που είναι άμεσα συνδεδεμένοι με τα log files.

/var/log/ossec/etc/ossec.conf

http://www.madirish.net/293

Έτσι κάθε αρχείο log χρειάζεται έναν decoder έτσι ώστε να αποκωδικοποιείται η μορφή των logs και να εξάγονται πεδία όπως source IP, time κλπ.

/var/ossec/etc/decoder.xml.

OSSEC.conf

Global

Μέσα στο τμήμα global (<global>…</global>) μπορούμε να διαμορφώσουμε τις γενικές ρυθμίσεις του OSSEC.

- Ειδοποίηση μέσω e-mail

  Ενεργοποιήσαμε την ειδοποίηση μέσω e-mail προσθέτοντας τα παρακάτω μέσα στο τμήμα global.

```
<global>
  <email_notification>yes</email_notification>
  <email_to>example@gmail.com</email_to>
  <smtp_server>alt2.gmail-smtp-in.l.google.com.</smtp_server>
  <email_from>ossecm@kali</email_from>
</global>
```

Με το παρακάτω τμήμα που προσθέσαμε στο OSSEC.conf αποστέλλονται στο email και αναφορές με τα logs του OSSEC.

```
<reports>
      <title>Anafores</title>
      <showlogs>yes</showlogs>
      <email_to>vlivadaros@gmail.com</email_to>
</reports>
```

OSSEC.conf

- Λίστα white list

  Μέσα στα tags <white_list> προσθέτουμε τις διευθύνσεις IP οι οποίες δεν θέλουμε να μπλοκαριστούν ποτέ από το OSSEC.

```
<global>
  <white_list>127.0.0.1</white_list>
  <white_list>^localhost.localdomain$</white_list>
  <white_list>192.168.196.2</white_list>
</global>
```

❖ Database Output

Το OSSEC μπορεί να αποθηκεύει τις εξόδους του, δηλαδή τις ειδοποιήσεις, τα logs κ.τ.λ., σε μια βάση δεδομένων. Οι βάσεις που υποστηρίζει για το σκοπό αυτό είναι οι MySQL και PostgreSQL.
Το τμήμα Database Output χρησιμοποιείται για τη δήλωση των στοιχείων της βάσης αυτής, όπως φαίνεται παρακάτω:

```
<database_output>
  <hostname>192.168.132.134</hostname>
  <username>root</username>
  <password>toor</password>
  <database>test</database>
  <type>mysql</type>
</database_output>
```

OSSEC.conf

Rules

Το OSSEC διαθέτει ένα σύνολο από κανόνες οι οποίοι είναι αρχεία .xml βρίσκονται στο φάκελο /var/OSSEC/rules/ . Εάν κάποιος θέλει να προσθέσει πιο ειδικούς κανόνες πρέπει να τους γράψει στο αρχείο «local_rules.xml» που βρίσκεται στον παραπάνω φάκελο. Τα υπόλοιπα .xml αρχεία του φακέλου αυτού δεν πρέπει να τροποποιηθούν.
Οι κανόνες αυτοί δηλώνονται στο OSSEC.conf μέσα στο τμήμα <rules>

```
<rules>
    <include>rules_config.xml</include>

                [...]

    <include>local_rules.xml</include>
</rules>
```

Syscheck

Το τμήμα <syscheck> περιλαμβάνει τις ρυθμίσεις ελέγχου του συστήματος για οποιαδήποτε αλλαγή στα αρχεία και τους φακέλους του συστήματος.

OSSEC.conf

- Συχνότητα

  Για να ρυθμίσουμε την συχνότητα εκτέλεσης του syscheck πρέπει να γράψουμε το χρόνο που θέλουμε, σε δευτερόλεπτα, μέσα στο tag <frequency>

```
<syscheck>

   <frequency>300</frequency>
             [...]

</syscheck>
```

- Φάκελοι που ελέγχονται

  Στη συνέχεια καθορίζουμε τους φακέλους τους οποίους θα ελέγχει το syscheck και θα μας ειδοποιεί για οποιαδήποτε αλλαγή

```
<syscheck>

             [...]
  <directories realtime="yes" check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
  <directories realtime="yes" check_all="yes">/bin,/sbin</directories>
             [...]

</syscheck>
```

OSSEC.conf

- Φάκελοι και αρχεία που αγνοούνται

Εάν δεν επιθυμούμε το OSSEC να μας ειδοποιεί για κάποια συγκεκριμένα αρχεία ή φακέλους τότε τα βάζουμε μέσα στο <ignore> tag, όπως φαίνεται παρακάτω

```
<!-- Files/directories to ignore -->
<ignore>/etc/mtab</ignore>
<ignore>/etc/mnttab</ignore>
<ignore>/etc/hosts.deny</ignore>
<ignore>/etc/mail/statistics</ignore>
<ignore>/etc/random-seed</ignore>
<ignore>/etc/adjtime</ignore>
<ignore>/etc/httpd/logs</ignore>
<ignore>/etc/utmpx</ignore>
<ignore>/etc/wtmpx</ignore>
<ignore>/etc/cups/certs</ignore>
<ignore>/etc/dumpdates</ignore>
<ignore>/etc/svc/volatile</ignore>
```

- Rootcheck

Στο τμήμα <syscheck> ανήκει και ο έλεγχος rootcheck αν και δεν εμπεριέχεται μέσα στο tag του syscheck και είναι σε ξεχωριστό tag. Το rootcheck ψάχνει να βρει αν υπάρχουν rootkits μέσα στο σύστημα.

```
 <rootcheck>
   <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
   <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
   <system_audit>/var/ossec/etc/shared/system_audit_rcl.txt</system_audit>
   <system_audit>/var/ossec/etc/shared/cis_debian_linux_rcl.txt</system_audit>
   <system_audit>/var/ossec/etc/shared/cis_rhel_linux_rcl.txt</system_audit>
   <system_audit>/var/ossec/etc/shared/cis_rhel5_linux_rcl.txt</system_audit>
<frequency>300</frequency>
 </rootcheck>
```

OSSEC.conf

- **Alerts**

Οι κανόνες του OSSEC έχουν ένα επίπεδο σημαντικότητας (level) το οποίο κυμαίνεται από 0 (το πιο ασήμαντο) έως 16 (το πιο σημαντικό). Στο τμήμα <alerts> δηλώνουμε από ποιο επίπεδο και πάνω θέλουμε να μας ειδοποιεί το OSSEC για τους αντίστοιχους κανόνες

```
<alerts>
  <log_alert_level>1</log_alert_level>
  <email_alert_level>1</email_alert_level>
</alerts>
```

Έχουμε ρυθμίσει το OSSEC να γράφει στο αρχείο /var/OSSEC/logs/alerts/alerts.log ειδοποιήσεις για κανόνες επιπέδου 1 και πάνω (<log_alert_level>1</log_alert_level>) και να στέλνει ειδοποιήσεις στο email που δηλώσαμε για κανόνες επιπέδου 1 και πάνω (<email_alert_level>1</email_alert_level>)

https://www.ossec.net/docs/manual/rules-decoders/rule-levels.html

OSSEC.conf

Active-response/Command

Στο τμήμα αυτό ανήκουν τα <active-response> και τα <command> tags

```
<ossec_config>
    <command>
        <!--
        Command options here
        -->
    </command>
    <active-response>
        <!--
        active-response options here
        -->
    </active-response>
</ossec_config>
```

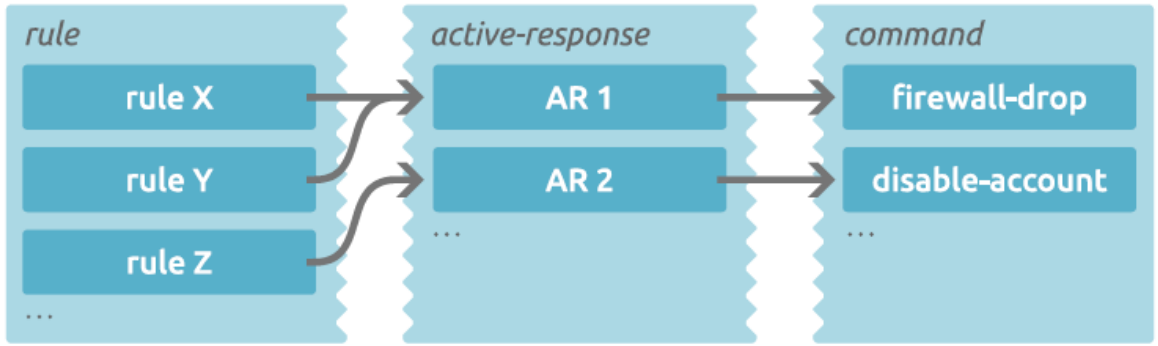
- Commands

Τα εκτελέσιμα αρχεία των commands βρίσκονται στο φάκελο /var/OSSEC/active-response/bin/. Για την προσθήκη νέων commands, αφού γράψουμε τον κώδικα, αποθηκεύουμε το αρχείο ως .sh στον παραπάνω φάκελο. Στη συνέχεια το δηλώνουμε στο OSSEC.conf.

OSSEC.conf

- Active-response

  Τα active-response λειτουργούν ως σύνδεσμοι ανάμεσα στα rules και commands.
  Οι rules πυροδοτούν τα active-response τα οποία στη συνέχεια ειδοποιούν
  τα αντίστοιχα commands να ξεκινήσουν την εκτέλεση τους



Collector

Στο τέλος του αρχείου OSSEC.conf υπάρχουν τα tags <localfile>

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/messages</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>
```

Στο τμήμα αυτό δηλώνονται τα αρχεία που θέλουμε να παρακολουθεί το OSSEC.
Τα αρχεία αυτά είναι συνήθως τα αρχεία καταγραφής του εκάστοτε συστήματος.