GUIDA ALL'INSTALLAZIONE DI UN SENSORE PER IL RILEVAMENTO E L'ANALISI DELLE INTRUSIONI SU SISTEMI INFORMATICI

10-01-2004 by ClaudioVe, Profex, S.Teggi – http://www.casalelinux.org

---

Sistema di test CPU: AMD 1000 mhz RAM: 512 mb	Sistema Operativo Linux “Fedora”

PREMESSA:

Il seguito di questa documentazione prenderà in esame i passaggi fondamentali per l'installazione del software necessario all'implementazione di un sistema locale di rilevamento delle intrusioni su sistemi informatici e la sua configurazione.
Questo lavoro è il risultato della lettura di diversa documentazione reperibile su internet, dove però abbiamo rilevato molte “leggerezze” o passaggi dati per scontati e non documentati, che possono disorientare e bloccare chi si approccia a questo lavoro con conoscenze non elevate.

Abbiamo optato di documentare i passaggi utilizzando i software in esame in formato “sorgente”, per permettere la massima portabilita di questo documento su ogni sistema che ne consenta l'uso, fermo restando che le varie pacchettizzazioni binarie che utilizzano alcune distribuzioni potranno svolgere altrettanto bene il lavoro e forse anche più velocemente (in questo caso fate riferimento alla documentazione della distribuzione utilizzata).

Le prove sono state eseguite sulla stessa macchina, utilizzando diversi hard disk per permettere di testare il lavoro con le principali distribuzioni e in dettaglio abbiamo lavorato con:

FEDORA
REDHAT 9.0
MANDRAKE 9.1
SUSE 9.0
SLACKWARE 9.1

Queste distribuzioni sono state installate ex-novo scegliendo una configurazione minimalista che potesse evidenziare eventuali mancanze di pacchetti e librerie non necessarie all'uso normale di un sistema **GNU/Linux.**

L'implementazione di un sistema di rilevazione e analisi delle intrusioni informatiche così come spiegheremo tra poco prevede l''interazione di diversi software e la presenza di alcuni componenti base di GNU/Linux.
In dettaglio sono stati utilizzati :

acid-0.9.6b23 http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html

adodb372 http://php.weblogs.com/adodb#downloads

apache-1.3.29 http://www.apache.inetcosmos.org/dist/

gd-1.8.4 http://www.boutell.com/gd/

jpegsrc.v6b http://www.ijg.org/files/

jpgraph-1.14 http://www.aditus.nu/jpgraph/jpdownload.php

libpng-1.2.5 http://www.libpng.org/pub/png/libpng.html

mod_ssl-2.8.16-1.3.29 http://www.modssl.org/

mysql-standard-4.0.16-pc-linux-i686 http://www.mysql.com/

openssl-0.9.6l http://www.openssl.org/source/

php-4.3.4 http://www.php.net/downloads.php

phplot-4.4.6 http://sourceforge.net/project/showfiles.php?group_id=14653

snort-2.0.5 http://www.snort.org/dl

snortrules-stable http://www.snort.org/dl/rules

zlib-1.2.1 http://www.gzip.org/zlib

Verificate la presenza di nuove versioni dei sorgenti elencati che potrebbero sicuramente essere state rilasciate dopo la stesura di questo documento e che probabilmente risolvono alcuni problemi o bachi più o meno gravi.

PREREQUISITI:

Dovendo compilare i sorgenti sul nostro sistema e di fondamentale importanza verificare la presenza degli strumenti di compilazione/sviluppo che sono presenti su ogni distribuzione e in particolare del compilatore **gcc.** Se non presente procediamo con l'installzione di questo software.

Per comodità vi consigliamo di scompattare i pacchetti da utilizzare in una directory temporanea.
In questa guida useremo **/usr/local/file_acid** che creeremo con:

mkdir /usr/local/file_acid

Come per qualsiasi operazione sul nostro sistema operativo, è consigliabile oltre all'uso di questa guida, la verifica delle procedure contenute nei vari file README, INSTALL o simili contenuti nei pacchetti dei programmi.
Assicuratevi di rimuovere eventuali versioni dei software che useremo, già installate sul vostro sistema.
Per poter compliare i pacchetti richiesti correttamente sul sistema devono essere presenti alcune librerie fondamentali.
Verificate la presenza di **zlib, libpng e jpegsrc** e in caso negativo procedete all'installazione come segue.

PREPARAZIONE DEL SISTEMA:

pre_0.1 – Installazione di zlib

```
cd /usr/local/file_acid
tar zxvf zlib-1.2.1.tar.gz
cd zlib-1.2.1
./configure
make test
make install
```

pre_0.2 – Installazione di libpng

```
cd /usr/local/file_acid
tar zxvf libpng-1.2.5.tar.gz
cd libpng-1.2.5
cp scripts/makefile.linux Makefile
make test
make install
```

pre_0.3 – Installazione di jpegsrc

```
cd /usr/local/file_acid
tar zxvf jpegsrc.v6b.tar.gz
cd jpeg-6b
./configure
make
make test
make -n install
```

Terminata la preparazione del sistema, possiamo procedere con l'installazione e la configurazione dei software necessari alla...

COSTRUZIONE DEL SISTEMA IDS (Intrusion Detection System)

1.1 - Installazione di gd

```
cd /usr/local/file_acid
tar zxvf gd-1.8.4.tar.gz
cd gd-1.8.4
make
(In caso di errori di headers mancanti, aprite il Makefile e inserite il
percorso dove trovare i file necessari. Ad es. potrebbe
indicare:d_jpeg.c:26:21: jpeglib.h: No such file or directory
...
Quindi cerchiamo la sezione header nel Makefile:
INCLUDEDIRS=-I. -I/usr/include/freetype2 -I/usr/include/X11 -I/
usr/X11R6/include/X11 -I/usr/local/include
ed aggiungiamo il path dove cercare gli header necessari, in questo
caso:
-I/usr/local/file_acid/jpeg-6b)


make install
```

1.2 – Installazione di mysql

```
cd /usr/local/file_acid
tar zxvf mysql-standard-4.0.16-pc-linux-i686.tar.gz
cd mysql-standard-4.0.16-pc-linux-i686
groupadd mysql
useradd -g mysql mysql
cd /usr/local/
ln -s /usr/local/file_acid/mysql-standard-4.0.16-pc-linux-i686 mysql
cd mysql
scripts/mysql_install_db
chown -R root  .
chown -R mysql data
chgrp -R mysql .
bin/mysqld_safe --user=mysql & (anche bin/safe_mysqld --user=mysql &)
bin/mysqladmin -u root password 'setta una password per l'user root di
mysql'
```

1.3 - openssl

```
cd /usr/local/file_acid
tar zxvf openssl-0.9.6l.tar.gzcd openssl-0.9.6l
cd openssl-0.9.6l
sh config \ no-idea \ no-threads \ -fPIC
make depend
make

make install
```

1.4 - Preparazione di apache

```
cd /usr/local/file_acid
tar zxvf apache_1.3.29.tar.gz
cd apache-1.3.29
./configure --prefix=/usr/local/apache
```

1.5 – Installazione di mod_ssl

```
cd /usr/local/file_acid
tar -zxvf mod_ssl-2.8.16-1.3.29.tar.gz
cd mod_ssl-2.8.16-1.3.29
./configure --with-apache=../apache_1.3.29 --with-ssl=../openssl-0.9.6l --
prefix=/usr/local/apache --enable-shared=ssl --enable-module=ssl --
enable-rule=SSL_EXPERIMENTAL --enable-rule=SSL_VENDOR --enable-
rule=EAPI --enable-rule=SSL_SDBM
```

1.6 – Completiamo l'installazione di apache

```
cd /usr/local/file_acid/apache-1.3.29
make
make certificate

(IMPORTANTE!!! A questo punto vi veerranno chiesti i dati per la
compilazione del certificato.
Potete impostare:
Signature Algorithm: Select RSA (default)
Certificate version: Select 3 (default)
Encrypt private Key: selezionate NO se non volete la richiesta della
password all'avvio di apache,
selezionate YES se invece volete avviare il server web tramite
autenticazione


make install
```

1.7 – Modifichiamo il file di configurazione di apache

Apriamo con un editor il file di configurazione del server web apache:
/usr/local/apache/conf/httpd.conf

```
        MinSpareServers    5
                MaxspareServers   10
          StartServer        5
          MaxClients        10
          Port          443
          ServerSignature   Off
```

Se non desiderate che il server web resti in ascolto sulla porta 80 decommentate o cancellate:

```
          Listen        80
```

Aggiungete le seguenti istruzioni mime.type

```
          AddType application/x-httpd-php .php .php3
          AddType application/x-httpd-php-source .phps .phps3
          AddType image/x-icon .ico
```

e quindi:

```
DirectoryIndex index.html index.php index.php3
```

1.8 – Installazione di php

```
cd /usr/local/file_acid
tar zxvf php-4.3.4
cd php-4.3.4
./configure --prefix=/usr/local/apache/php --with-mysql=/usr/local/mysql --with-apxs=/usr/local/apache/bin/apxs --with-zlib-dir=/usr/local --enable-bcmath --with-gd --enable-sockets --enable-track-vars
make
make install
cp php.ini-dist /usr/local/lib/php.ini
```

1.9 – Impostiamo il database di snort

```
cd /usr/local/mysql
bin/mysql -p
<pass impostata al punto "1.2">
\u mysql
DELETE FROM user WHERE User='';
DELETE FROM user WHERE Password='';
GRANT ALL PRIVILEGES ON *.* TO dba@localhost IDENTIFIED BY
'settiamo_una_password';
CREATE DATABASE snort;
GRANT INSER,SELECT,DELETE ON snort.* TO snort@localhost
IDENTIFIED BY 'settiamo_una_password';

\q
```

2.0 – Installiamo jpgraph

```
cd /usr/local/file_acid
tar zxvf jpgraph-1.14.tar.gz
mv jpgraph-1.14 /usr/local/apache/htdocs/jpgraph
cd /usr/local/apache/htdocs/jpgraph
rm -rf README
rm -rf QPL.txt
```

2.1 – Installiamo e impostiamo acid

```
cd /usr/local/file_acid
tar -zxvf acid-0.9.6b23.tar.gz
mv acid /usr/local/apache/htdocs/
chmod 0775 /usr/local/apache/htdocs/acid/
chmod 0644 /usr/local/apache/htdocs/acid/*
chown -R root:wheel /usr/local/apache/htdocs/acid/*
```

2.2 – Installiamo e impostiamo adodb

```
cd /usr/local/file_acid
tar -zxvf adodb372.tgz
mv adodb /usr/local/apache/htdocs/
chmod 0775 /usr/local/apache/htdocs/adodb/
chmod 0644 /usr/local/apache/htdocs/adodb/*

chown -R root:wheel /usr/local/apache/htdocs/adodb/*
```

2.3 – Installiamo e imposti phplot

```
cd /usr/local/file_acid
tar -zxvf phplot-4.4.6.tar.gz
mv phplot-4.4.6 /usr/local/apache/htdocs/phplot
chmod 0775 /usr/local/apache/htdocs/phplot/
chmod 0644 /usr/local/apache/htdocs/phplot/*
chown -R root:wheel /usr/local/apache/htdocs/*
```

2.4 – Installiamo snort

```
cd /usr/local/file_acid
tar -zxvf snort-2.0.5.tar.gz
cd /usr/local
ln -s /usr/local/file_acid/snort-2.0.5 snort
cd snort
./configure --with-mysql=/usr/local/mysql --with-openssl=/usr/local/ssl
make
make install
```

2.5 – Creiamo il database di snort

```
cd /usr/local/mysql
bin/mysql -u dba -p snort </usr/local/file_acid/snort-
2.0.5/contrib/create_mysql
gunzip /usr/local/file_acid/snort-2.0.5/contrib/snortdb-extra.gz
bin/mysql -u dba -p snort </usr/local/file_acid/snort-2.0.5/contrib/snortdb-
extra

bin/mysql -u dba -p snort
</usr/local/apache/htdocs/acid/create_acid_tbls_mysql.sql
```

2.6 – Verifica del database

```
cd /usr/local/mysql
bin/mysql -p
mysql> SHOW DATABASES;
(dobbiamo vedere un database: mysql, snort e test)
mysql> use snort;
mysql> SHOW TABLES;
(dobbiamo vedere una lista di 23 tabelle)
\q
```

2.7 – Configuriamo acid

Apriamo con un editor il file:
/usr/local/apache/htdocs/acid/acid_conf.php
e impostiamo le seguenti voci:

```
$DBlib_path = "/usr/local/apache/htdocs/adodb";
$DBtype = "mysql";
$ChartLib_path = "/usr/local/apache/htdocs/jpgraph/src";

$alert_dbname   = "snort";
$alert_host     = "localhost";
$alert_port     = "3306";
$alert_user     = "root";
$alert_password = "settiamo_una_password”;

$archive_dbname   = "snort";
$archive_host     = "localhost";
$archive_port     = "3306";
$archive_user     = "root";
$archive_password = "settiamo_una_password";
```

2.8 – Configuriamo snort.conf

```
cd /usr/local
ln -s /usr/local/file_acid/snort-2.0.5 snort
cd snort
cd /usr/local/file_acid/snortrules-current.tar.gz
tar zxvf snortrules-current.tar.gz -C /usr/local/snort
cd /usr/local/snort/rules
vi snort.conf
output database: alert, mysql, dbname=snort user=snort host=localhost
password=settiamo_una_password sensor_name=settiamo_un_nome
cp usr/local/snort/rules/snort.conf usr/local/snort/etc/snort.conf
```

2.9 - Creiamo la directory per i log di snort

```
#mkdir /var/log/snort
```

Stoppiamo e riavviamo i servizi httpd & mysqld (adottare il metodo della propria distribuzione per la gestione dei servizi!) e proviamo a lanciare snort:
 # snort -dev -c /usr/local/snort/etc/snort.conf
Se tutto Ã¨ a posto dovremmo vedere qualcosa del genere:
…
--== Initialization Complete ==--

-*> Snort! <*-
Version 2.0.5 (Build 98)

By Martin Roesch (roesch@sourcefire.com, www.snort.org)
...

Apriamo una sessione X e putniamo un browser su
https://localhost/acid
Se funziona dovremmo vedere la home page di Acid...

...buon divertimento!