Secure
Snort, ACID, Base Howto

1. Snort, ACID, Oinkmaster und Guardian Howto auf Debian 4.0:

Vorrausetzungen:
MySQL, Apache2, PHP4

Erstellen Sie zuerst die Datenbank snort und den User snort in MySQL.
Der user snort sollte alle rechte auf der DB haben.

1.1. Snort installieren Download von: http://www.snort.org/dl/

Oinkmaster download von http://oinkmaster.sourceforge.net/ oder per apt-get

Build:
apt-get install libpcap0.8 libpcap0.8-dev php4-pear snort-mysql

Nur nötig bei manueler installation.
./configure --prefix=/opt/snort --with-mysql=/usr/lib/mysql

make
make install
mysql -u snort -p snort < contrib/create_mysql
zcat create_mysql.gz | mysql -u snort -pciw_snort snort

1.2. JPGraph installierenDownload von:
http://www.aditus.nu/jpgraph/jpdownload.php

Installation:

Entpacken in /var/www

ln -s jpgraph-version jpgraph

Das Linken ist praktisch bei späteren Updates, so muß nur der Link geändert werden.

1.3. ADODB installierenDownload von:

Installation:

Entpacken in /var/www

1.4. ACID installierenDownload von: http://acidlab.sourceforge.net/

Entpacken in /var/www

vi /var/www/acid/acid_conf.php

```
$DBlib_path = "/var/www/adodb";
$DBtype = "mysql";

$alert_dbname   = "snort";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "snort";
$alert_password = "password";

/* Archive DB connection parameters */
$archive_dbname   = "snort";
$archive_host     = "localhost";
$archive_port     = "";
$archive_user     = "snort";
$archive_password = "password";

/* ich fahr nich so auf pconnect ab */
$db_connect_method = 2;

$ChartLib_path = "/var/www/jpgraph/src";
```

pconnect

Eigendlich keine schlechte idee, wir mussten aber die Erfahrung machen das 99% der entwickler (die Datenbank wurde mitbenutzt für andere Firmen Projekte), zu hirn verbrannt sind um mit pconnect richtig umzugehen, so dass wir dies anschliessend verboten haben, ich habe mich dran gewöhnt und verwende pconnect nicht mehr.

Bei MySQL ist ein connect auch ausreichend schnell, so das es kaum wirkliche gründe für pconnect gibt.

1.5. Snort konfigurieren und zum starten fertig machen/opt/snort/etc/snort.conf

```
var HOME_NET            [213.133.103.207/32]
var EXTERNAL_NET        !$HOME_NET

var DNS_SERVERS         $HOME_NET
var SMTP_SERVERS        $HOME_NET
var HTTP_SERVERS        $HOME_NET
var SQL_SERVERS         $HOME_NET
var TELNET_SERVERS      $HOME_NET

var HTTP_PORTS          80:82
var SHELLCODE_PORTS     !80

var RULE_PATH /opt/snort/etc/rules

preprocessor frag2
```

```
preprocessor stream4:                detect_scans, disable_evasion_alerts
preprocessor stream4_reassemble:       both
preprocessor http_decode:              80 unicode double_encode full_whitespace
preprocessor rpc_decode:               111 32771
preprocessor bo
preprocessor telnet_decode
preprocessor portscan:               $HOME_NET 4 3 portscan.log
#preprocessor portscan-ignorehosts:     0.0.0.0

output database: log, mysql, user=snort password=xxxxx dbname=snort
host=localhost
output database: alert, mysql, user=snort password=xxxxx dbname=snort
host=localhost

include /opt/snort/etc/classification.config
include /opt/snort/etc/reference.config

include /opt/snort/etc/rules.conf
```

So sieht es bei mir aus, Sie werden sicherlich das ein oder andere anpassen müssen/wollen.
Mindestens aber den Netzbereich für $HOME_NET und die MySQL Zugangsdaten.

Etweige Rules die ich haben möchte werden über rules.conf inkludiert.
Die classification.config und reference.config finden Sie im snort Source Directoty unter /etc.

/opt/snort/etc/run

```
#!/bin/sh
SNORT_BIN="/opt/snort/bin/snort"
SNORT_OPTS=" -c /opt/snort/etc/snort.conf -i eth0 -u snort -g snort -l /log -t
/opt/snort/run"
exec $SNORT_BIN $SNORT_OPTS
```

Oinkmaster:

```
touch /etc/autodisable.conf
cd /usr/local/src/
wget http://mesh.dl.sourceforge.net/sourceforge/oinkmaster/oinkmaster-2.0.tar.gz

tar –zxvf oinkmaster-2.0.tar.gz
cd oinkmaster-2.0
cp oinkmaster.pl /usr/bin
cp oinkmaster.conf /etc/
cd contrib.
cp makesidex.pl /etc
chown -R snort:snort /etc/snort
mcedit /etc/oinkmaster.conf
```

url = http://www.snort.org/pub-bin/oinkmaster.cgi/oinkcode /snortrules-snapshot-2.3.tar.gz

```
 cd /etc
  ./makesidex.pl /etc/snort/rules >autodisable.conf
  mkdir /etc/snort/backup
  chown -R snort:snort /etc/snort/backup
  cd /usr/bin
  touch oinkdaily
  chmod +x oinkdaily
  mcedit oinkdaily

  I added the following line to the oinkdaily file
  oinkmaster.pl -C /etc/oinkmaster.conf -C /etc/autodisable.conf -o /etc/snort/rules -b
  /etc/snort/backup 2>&1 | mail -s "oinkmaster" hkiyimbabou.or.ug

  Then I scheduled snort to download the rules

  crontab –u snort –e
  30 5 * * * /usr/bin/oinkdaily

  Any help will be appreciated


pear channel-update pear.php.net
pear upgrade-all

apt-get install php5-gd
pear install Numbers_Roman-1.0.2
install ok: channel://pear.php.net/Numbers_Roman-1.0.2

pear install Numbers_Words-0.15.0
install ok: channel://pear.php.net/Numbers_Words-0.15.0

pear install Image_Color-1.0.2.tgz
install ok: Image_Color 1.0.2

pear install Image_Canvas-0.3.0.tgz
install ok: Image_Canvas 0.3.0

pear install Image_Graph-0.7.2.tgz
Optional dependencies:
package `Numbers_Roman' is recommended to utilize some features.
package `Numbers_Words' is recommended to utilize some features.
install ok: Image_Graph 0.7.2
```

Secure

Eindeutige ID: #1019
Verfasser: Michael Stender
Letzte Änderung: 2008-06-29 00:05