Установка Snort

Snort, Apache, PHP, MySQL and BASE Install on SuSe 9.2

BASE - Basic Analysis and Security Engine

Исходные данные:

Hardware:
IBM xSeries 335, CPU Xeon 2,8 MHz, 2,5 GB RAM, 70GB SCSI Hot-swap HDD (RAID-1), Ethernet 10/100/1000

Software:
SuSe Linux 9.2, kernel 2.6.8-24.5-smp

Установка SuSe 9.2:

Установка в основном проходит с параметрами по-умолчанию.

Язык и клавиатура: English

Устанавливаем статический ip-адрес для одного из интерфейсов, например eth0

Отключаем файрвол.

Конфигурация пакетов: на основе Standart system with KDE, дополнительно устанавливаем следующие пакеты:

- Expect 5.41-2
- Ethereal 0.10.6-3
- Nmap 3.70-2
- Gd 2.0.28-2.3
- Libpng-devel 1.2.6-4
- Libpng 1.2.6-4
- Libpcap 0.8.3-3
- Zlib 1.2.1
- Libjpeg 6.2.0
- Gcc 3.3.4
- Lynx 2.8.5-32
- Flex 2.5.4a-295
- Pcre-devel 4.5.2
- Termcap 2.0.8-878
- Ncurses-devel 5.4
- Gcc-c++ 3.3.4

Установка времени: выставляем корректно время

Система по-умолчанию запускается на 3м уровне.

После установки:

Через yast запускаем on-line обновление.

Отключаем неиспользуемые сервисы:
chkconfig –d isdn
chkconfig –d portmap
chkconfig –d isdn
chkconfig –d cups
chkconfig –d nfs
chkconfig –d nfsboot
chkconfig –d smbfs
chkconfig –d powersaved
chkconfig –d ypbind

Отключаем все сервисы запускаемые через xinetd (по-умолчанию все отключено), можно сделать через yast

Изменение конфигурации SSH, редактируем файл /etc/ssh/sshd_config:

Protocol 2
PermitRootLogin no
PermitEmptyPasswords no

Закачиваем файлы необходимые для установки SNORT:

Download Snort 2.2.0
http://www.snort.org/dl/snort-2.2.0.tar.gz

Download ADODB 4.54
http://adodb.sourceforge.net/

Download BASE 1.0
http://base.secureideas.net/

Download JPGraph 1.16
http://www.aditus.nu/jpgraph/downloads/jpgraph-1.16.tar.gz

Download Apache 2.0.52
http://httpd.apache.org/

Download PHP 4.3.9
http://www.php.net/

Download MySQL 4.0.20
http://www.mysql.ru/cgi-bin/download/mysql-4.0.20.tar.gz

Download Oinkmaster 1.1
http://oinkmaster.sourceforge.net/download.shtml

Download Webmin 1.170
http://prdownloads.sourceforge.net/webadmin/webmin-1.170.tar.gz

Инсталяция MySQL:

В директории /root редактируем файл.bash_profile:

PATH=$PATH:$HOME/bin:/usr/local/mysql/bin
export PATH

Или создаем новые добавив в начало файла заголовок (без кавычек)
“# .bash_profile”

Копируем mysql-4.0.20.tar.gz в /tmp/1

groupadd mysql
useradd -g mysql mysql
cp mysql-4.0.20.tar.gz /tmp/1/
cd /tmp/1
tar –xvzf mysql-4.0.20.tar.gz
cd mysql-4.0.20
./configure --prefix=/usr/local/mysql
make
make install
scripts/mysql_install_db
chown -R root /usr/local/mysql
chown -R mysql /usr/local/mysql/var
chgrp -R mysql /usr/local/mysql
cp support-files/my-medium.cnf /etc/my.cnf
cp support-files/mysql.server /etc/init.d/mysql
chown root.root /etc/init.d/mysql
chmod 755 /etc/init.d/mysql
chkconfig –add /etc/init.d/mysql

Добавляем в файл /etc/ld.so.conf строки (без кавычек)
“/usr/local/mysql/lib/mysql”
“/usr/local/lib ”

Выполняем
ldconfig –v

Инсталяция Apache и PHP:

Копируем httpd-2.0.52.tar.gz в /tmp/2

cp httpd-2.0.52.tar.gz /tmp/2/
cd /tmp/2
tar -xvzf httpd-2.0.52.tar.gz
cd httpd_2.0.52
./configure –prefix=/srv/www --enable-so
make

make install
/srv/www/bin/apachectl start

Проверяем что Apache запустился, заходим браузером.

/srv/www/bin/apachectl stop

Создаем скрипт автозапуска (см. приложение 1), кладем его в /etc/init.d.

cd /etc/init.d
chkconfig -add apache2

Копируем php-4.3.9.tar.tar в /tmp/3

cp php-4.3.9.tar.tar /tmp/3/
cd /tmp/3
tar -xvzf php-4.3.9.tar.tar
cd php-4.3.3
./configure --prefix=/srv/www/php --with-apxs2=/srv/www/bin/apxs --with-config-file-path=/srv/www/php --enable-sockets --with-mysql=/usr/local/mysql --with-zlib --with-gd (одной строкой)
make
make install
cp php.ini-dist /srv/www/php/php.ini

Редактируем /srv/www/conf/httpd.conf, добавляем или редактируем следующие строки:

LoadModule php4_module modules/libphp4.so
AddType application/x-tar .tgz
AddType image/x-icon .ico
AddType application/x-httpd-php .php
DirectoryIndex index.php index.html index.html.var

Apache инсталируется в /srv/www. Для проверки работы Apache, создаем файл /srv/www/htdocs/test.php содержащий строку “<?php phpinfo(); ?>” (без кавычек). Стартуем Apache
/ect/init.d/apache2 start
заходим браузером http://IP_Addess/test.php

Инсталируем SNORT:

Копируем snort-2.2.0.tar.gz в /tmp/4

cp snort-2.2.0.tar.gz /tmp/4/
cd /tmp/4
groupadd snort
useradd -g snort snort
tar -xvzf snort-2.2.0.tar.gz

```
# cd snort-2.2.0
# ./configure --with-mysql=/usr/local/mysql
# make
# make install
# mkdir /etc/snort
# mkdir /var/log/snort
# cd rules
```

делаем следующий блок для каждого интерфейса где должен быть запущен snort, ethx – x номер интерфейса

```
# mkdir /etc/snort/ethx
# mkdir /var/log/snort/ethx
# cp * /etc/snort/ethx
# cd ../etc
# cp snort.conf /etc/snort/ethx
# cp *.config /etc/snort/ethx
# cp unicode.map /etc/snort/ethx
# cp threshold.conf /etc/snort/ethx
# cd ..
```

Создаем скрипт автозапуска (см. приложение 2), кладем его в /etc/init.d.

```
# cd /etc/init.d
# chown root.root /etc/init.d/snort
# chmod 755 /etc/init.d/snort
# chkconfig -add snort
```

Редактируем
INTERFACES="eth***x*** eth***y***"

Редактируем каждый /etc/snort/ethx/snort.conf file:

var HOME_NET $ethx_ADDRESS (ethx - номер интерфейса который будем мониторить)
или
var HOME_NET сеть/маска
var RULE_PATH /etc/snort/ethx (указываем где храняться правила)
output database: log, mysql, user=snort password=***new_password*** dbname=snort host=localhost

В конце файла раскоментруем те правила которые необходимо включить

Устанавливаем скрипт автоматического обновления правил Oinkmaster:

```
# cp oinkmaster-1.1.tar.gz /tmp/5/
# cd /tmp/5
# tar –xvzf oinkmaster-1.1.tar.gz
# cd oinkmaster-1.1
# cp oinkmaster.pl /etc/snort/
# cp oinkmaster.conf /etc/snort/eth0/
```

…..
cp oinkmaster.conf /etc/snort/ethx/
cp oinkmaster.1 /usr/local/man/man.1/man1/

В зависимости от версии snort правим параметр url в файле /etc/snort/ethx/oinkmaster.conf

Устанавливаем базу данных в MySQL:

Запускаем mysql
/etc/init.d/mysql start
/usr/local/ mysql/bin/mysql

mysql> SET PASSWORD FOR root@localhost=PASSWORD('new_passwo rd');
>Query OK, 0 rows affected (0.25 sec)

mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)

mysql> grant INSERT,SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)

mysql> SET PASSWORD FOR snort@localhost=PASSWORD('new_password ');
>Query OK, 0 rows affected (0.25 sec)

mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)

mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
>Query OK, 0 rows affected (0.02 sec)

mysql> exit
>Bye

Переходим в директорию в которую развернули snort
cd /tmp/4
/usr/local/mysql/bin/mysql -u root -p < ./contrib/create_mysql snort
Enter password:
(Указываем пароль пользователя root (mysql))

Устанавливаем дополнительные таблицы:
zcat ./contrib/snortdb-extra.gz | /usr/local/mysql/bin/mysql -p snort
Enter password:

(Указываем пароль пользователя snort (mysql))
Проверяем что все таблицы создались корректно:

/usr/local/mysql/bin/mysql –p
>Enter password:

```
mysql> SHOW DATABASES;
(You should see the following)
+------------+
| Database
+------------+
| mysql
| snort
| test
+------------+
3 rows in set (0.00 sec)


mysql> use snort
>Database changed
mysql> SHOW TABLES;
+------------------+
| Tables_in_snort
+------------------+
| data
| detail
| encoding
| event
| flags
| icmphdr
| iphdr
| opt
| protocols
| reference
| reference_system
| schema
| sensor
| services
| sig_class
| sig_reference
| signature
| tcphdr
| udphdr
+------------------+
19 rows in set (0.00 sec)
>Bye
```

Инсталируем JPGraph:

Копируем jpgraph-1.16.tar.gz в /srv/www/htdocs

```
# cp jpgraph-1.16.tar.gz /srv/www/htdocs
# cd /srv/www/htdocs
```

```
# tar –xvzf jpgraph-1.16.tar.gz
# rm –rf jpgraph-1.16.tar.gz
```

Инсталируем ADODB:

Копруем adodb454.gz в /srv/www/htdocs

```
# cp adodb454.gz /srv/www/htdocs/
# cd /srv/www/htdocs
# tar -xvzf adodb454.gz
# rm –rf adodb454.gz
```

Инсталируем BASE:

Копируем base-1.0.tar.gz в /srv/www/htdocs

```
# cp base-1.0.tar.gz /srv/www/htdocs
# cd /srv/www/htdocs
# tar -xvzf  base-1.0.tar.gz
# rm -rf base-1.0.tar.gz
# cd base
# cp base_conf.php.dist base_conf.php
```

Редактируем /srv/www/htdocs/base/base_conf.php

```
$BASE_Language = “russian”;
$Use_Auth_System = 0;
$BASE_urlpath =  “/base”;
$DBlib_path = "/srv/www/htdocs/adodb";
$DBtype = "mysql";

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

$archive_dbname = "snort";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "snort";
$archive_password = "new_password ";

$ChartLib_path = "/srv/www/htdocs/jpgraph-1.16/src";

$chart_file_format = "png";
```

Запускаем apache, mysql, snort и заходим браузером по адресу http://yourhost/base/base_main.php.

При первом запуске будет предложена инициализировать БД, заходи в “Setup page”, нажимаем "Create BASE AG".

Заходим на http://yourhost/base/

Устанавливаем пароль на BASE:

```
# mkdir /srv/www/passwords
# /srv/www/bin/htpasswd -c /srv/www/passwords/passwords/passwords base
```

base – пользователь под которым будем обращаться к BASE.

Добавляем в /srv/www/conf/httpd.conf

```
<Directory "/srv/www/htdocs/base">
  AuthType Basic
  AuthName "SnortIDS"
  AuthUserFile /srv/www/passwords/passwords
  Require user base
 </Directory>
```

Now restart the http service (/etc/init.d/httpd restart) and next time you go to the acid webpage you will get a prompt for a username and password. (if you are running some of the anti-spyware features of software like spybot search and destroy you will get an error when trying to view this page, or any that require authentication)

Инсталируем дополнительный сенсор FW

Ставим mysql-devel и mysql-client

```
# ln -s /usr/lib/mysql/ /usr/local/lib/mysql
```

Распаковываем snort

```
# cd snort-2.2.0
# ./configure --with-mysql
…..
# /usr/local/mysql/bin/mysql –u root –p
mysql> SET PASSWORD FOR ‘snort’@’%’=PASSWORD('new_password');
>Query OK, 0 rows affected (0.25 sec)

mysql> exit;
>Bye
```

Инсталируем Webmin

```
# cp webmin-1.170.tar.gz /tmp/7/
```

```
# cd /tmp/7
# tar -xvzf webmin-1.170.tar.gz
# cd webmin-1.170
# ./setup.sh /usr/local/webmin
```

Инсталируем perl-Net_SSLeay 1.25-29 и openssl-devel 0.9.7d-25
perl-DBD-mysql 2.9004-2

Troubleshooting

If you are having trouble type the following
snort –c /etc/snort/snort.conf
It will give you output that will be helpful. It will tell you if you are having problems with rules or if you have a bad line in your conf file. If you do this and read the output you will be able to fix most of the problems I get e-mailed with.

Make sure that the line for MySQL in the snort.conf file is not wrapped or cut into two lines. I have seen this happen a lot.

Приложение 1.

```
#!/bin/sh
#
# /etc/init.d/apache2
#
### BEGIN INIT INFO
# Provides:                 apache2 httpd2
# Required-Start:             $local_fs $remote_fs $network
# X-UnitedLinux-Should-Start:   $named $time postgresql sendmail mysql ypclient

dhcp radiusd
# Required-Stop:              $local_fs $remote_fs $network
# X-UnitedLinux-Should-Stop:
# Default-Start:              3 5
# Default-Stop:               0 1 2 6
# Short-Description:            Apache2 httpd
# Description:                Start the httpd daemon Apache 2
### END INIT INFO

pname=apache2

apache_exe=/srv/www/bin/apachectl

#
# main part
#
case "$1" in
   start*)
      echo -n "Starting httpd2 "
      $apache_exe start
      ;;
   stop)
      echo -n "Shutting down httpd2 "
      $apache_exe stop
      ;;
   restart)
      $0 stop
      $0 start "$@"
      # Remember status and be quiet
      ;;
   *)
   cat >&2 <<-EOF
      Usage: $0 <command>
      where <command> is one of:
            start            - start httpd
            stop             - stop httpd (sendign SIGTERM to parent)
            restart          - stop httpd if running; start httpd
            help             - this screen

      EOF
   exit 1
esac


#!/bin/bash
# /etc/init.d/snort
### BEGIN INIT INFO
```

```
# Provides: snort
# Required-Start: apache2 mysql $network
# Required-Stop: mysql
# Default-Start: 3 5
# Default-Stop: 0 1 2 4 6
# short-Description: start and stop Snort
# Description: Network Intrusion Dectection
#
#  $JFW: snort_new,v 1.16 2003/11/29 14:51:37 tflat Exp $
#
#  Author:      James F. Wilkus         <james@unixninja.us>
#  About:       Snort Control Script
#               This script was written to handle multiple interfaces, and as a
#               frontend to oinkmaster.  For each interface in INTERFACES,
#               create a directory that contains all snort rules and configs.
#
#               Each interface has its own configuration files and rule
#               sets.  I needed a way to control different rule sets for each
#               interface.
#
#               Here is an example:
#
#               INTERFACES="rl0 fxp0"
#
#               /etc/snort
#                       oinkmaster.pl
#                       rl0/
#                               *.rules
#                               snort.conf
#                               oinkmaster.conf
#                       fxp0/
#                               *.rules
#                               snort.conf
#                               oinkmaster.conf
#
#
#
#  Usage:       rc.snort -i &lt;interface&gt; [ start | update | stop ]
#
#
#  Other:
#
#  oinkmaster is a snort signature management tool.  I highly suggest it.  You
#  can get it from:
#
#  http://www.snort.org/dl/contrib/signature_management/oinkmaster/oinkmaster-0.6.tar.gz
#
#  For use on SuSE/RedHat systems, copy this script to /etc/init.d and run:
#
# # chkconfig snort on
#

umask 022

SNORT_PATH=/usr/local/bin
SNORTDIR=/etc/snort
SNORTLOG=/var/log/snort
SNORTUSER=snort
SNORTGROUP=snort
```

```
INTERFACES="eth4 eth5"
OPTIONS="-D"

test -x $SNORT_PATH/snort || exit 0

start_snort()
{    for INT in ${INTERFACES}
     do
      unset SKIP
      PIDFILE="/var/run/snort_${INT}.pid"
      SNORTCONF="${SNORTDIR}/${INT}/snort.conf"
      if [ -f "${PIDFILE}" ]; then
        SPROC=$( cat ${PIDFILE} )
        SNORTPID=$( ps -p ${SPROC} | grep -v PID )
        if [ -z "${SNORTPID}" ]; then
          echo "Removing stale PID file for ${INT}."
          rm ${PIDFILE}
        else
          echo "Snort is still running on ${INT}, skipping!"
          SKIP=YES
        fi
      fi
      if [ "${SKIP}" != "YES" ]; then
        echo "Snorting ${INT}"
        ifconfig ${INT} up
        $SNORT_PATH/snort -I -i ${INT} -c ${SNORTCONF} -g ${SNORTGROUP} –l ${SNORTLOG}/${INT}
$OPTIONS
      fi
 done
}

oinkmaster()
{
 for INT in ${INTERFACES}
   do
    ${SNORTDIR}/oinkmaster.pl -C ${SNORTDIR}/${INT}/oinkmaster.conf -o ${SNORTDIR}/${INT}
 done
}

stop_snort()
{
 for INT in ${INTERFACES}
   do
    PIDFILE="/var/run/snort_${INT}.pid"
    if [ -f "${PIDFILE}" ]; then
      SPROC=$( cat ${PIDFILE} )
      echo "Stopping snort pid ${SPROC}"
      kill ${SPROC}
      rm ${PIDFILE}
    else
      echo "Snort is not running on ${INT}!"
    fi
   done
}

case $1 in
 start)
      start_snort ;;
 stop)
```

```
        stop_snort ;;
  update)
        echo "Updating Snort rules"
        oinkmaster ;;
  restart)
        $0 stop
        $0 start
        ;;
  *)
        echo "$0 [ start | stop | restart ]" ;;
esac
```