By Miguel Brams

Published: 2008-02-08 16:17

Intrusion Detection: Snort (IDS), OSSEC (HbIDS) And Prelude (HIDS) On Ubuntu Gutsy Gibbon

Everybody knows the problem, you have a IDS tool(s) installed and every tool has his own interface.

Prelude will allow to log all of the events to the prelude database and be consulted using one interface (prewikka). This howto will describe how to install and configure the different tools that will make up the complete solution.

This howto is based on bits and scraps I found in order to resolve some issues, parts from the manuals and my own experiance with installing the complete solution.

For more information on snort visit: **www.snort.org**

For more information on ossec visit: **www.ossec.net**

For more information on prelude visit: **www.prelude-ids.org**

Prerequisites:

Let's just assume you followed the **The Perfect Server - Ubuntu Gutsy Gibbon (Ubuntu 7.10)**. If not follow that howto and only install / add those part's you havent got installed on your system.

The following packages are useful, so please check that they are installed correctly:

```
apt-get install ntpdate
apt-get install dbconfig-common
```

Installing And Configuring Prelude

Normally, we would have to compile and install ***libprelude***, ***libpreludedb***, and then create the databases. Luckely enough the packages are provide by the Ubuntu repositories.

Prelude Manager

```
apt-get install prelude-manager
```

```
- Using default TLS settings from /etc/prelude/default/tls.conf:
  - Generated key size: 1024 bits.
  - Authority certificate lifetime: unlimited.
  - Generated certificate lifetime: unlimited.

  - Creating analyzer prelude-manager.
  - Creating /etc/prelude/profile/prelude-manager...
  - Allocated ident for prelude-manager: 4232957740008155.
  - Generating RSA private key... This might take a very long time.
  [Increasing system activity will speed-up the process.]

  - Generating 1024 bits RSA private key...
```

During the installation, the manager will create the profile for the ***prelude*** user. It can take a (very) long time, since GnuTLS tries to access ***/dev/random*** instead of ***/dev/urandom***(for security reasons). This may change in the future (maybe using anoption to have a faster generation, but crytographically less secure).

dbconfig will then ask you if you want it to configure the databaseautomatically. If you don't want to, just say no, and configureeverything manually (the sql scripts are in directory ***/usr/share/libpreludedb/***). Let's suppose the answer is yes.

Note: the number of questions may change, depending on debconf verbosity (set using ***dpkg-reconfigure debconf***), and dbconfig parameters, in file ***/etc/dbconfig-common/config.***

```
configure database with dbconfig-common: yes
database type:
```

Set the type to the database you previously installed. In this case `mysql`.

```
Database admin password: ******
```

dbconfig-common will ask for a password for the 'prelude'user. If you don't provide any (just pressing enter), it will generatea random one. Don't worry, the configuration file will be updateautomatically.

```
dbconfig-common: writing config to /etc/dbconfig-common/prelude-manager.conf

Creating config file /etc/dbconfig-common/prelude-manager.conf with new version
granting access to database prelude for prelude@localhost: success.
verifying access for prelude@localhost: success.
creating database prelude: success.
verifying database prelude exists: success.
populating database via sql...  done.
dbconfig-common: flushing administrative password
Starting Prelude Manager: prelude-manager.
```

The Ubunty package automaticallycreates the user and the database for prelude. If you want to change the password, do so first in mysql and after in ***/etc/prelude-manager/prelude-manager.conf***.

Prelude-Manager should now be running:

```
ps auxw | grep manager
```

```
prelude 28530  0.0  0.1  59384  4480 ?        Ssl  13:49   0:00 /usr/sbin/prelude-manager
```

The first part is over, you now have a manager up and running.

Listen address:

The default listen address is localhost (127.0.0.1). This means that you have to change this to add sensors on different hosts in order for the agents to be able to reach the prelude-manager.

Edit ***/etc/prelude-manager/prelude-manager.conf***:

```
listen = xxx.xxx.xxx.xxx
```

Restart the server, and check the address (if you changed the address):

```
# /etc/init.d/prelude-manager stop
```

```
   Stopping Prelude Manager: prelude-manager.
```

```
# /etc/init.d/prelude-manager start
```

```
Starting Prelude Manager: prelude-manager.
```

```
# netstat -pantu | grep prelude
```

```
tcp        0      0 192.168.66.1:4690          0.0.0.0:*      LISTEN     30544/prelude-manager
```

Prelude-LML

You need to install ***prelude-lml*** on every host you want to monitor. Prelude-LML will analyze your logs and reports event to the managers.

```
# apt-get install prelude-lml
```

```
...
Starting Prelude LML: prelude-lml.
```

Before it can be used, two things needs to be done:

- The address of the manager must be configured on the lml
- The manager won't trust sensors, until they are registered

Manager address

If you changed the address the manager is listening on, you need to change the address in the client config on every machine you install ***prelude-lml*** .

The adress of the manager is stored in file ***/etc/prelude/default/client.conf***:

```
[prelude]
server-addr = 127.0.0.1
```

Registering the sensor

Registering the sensor is a four-step process, which requires to run commands on both the sensor and the manager:

On the LML client, run the register command:

```
prelude-adduser register prelude-lml "idmef:w" <manager address> --uid 0 --gid 0
```

Tip: if you don't remember the command, just run ***prelude-lml***. Since it is not registered, it will fail, but is smart enough to display the help:

```
# prelude-lml
- Subscribing plugin pcre[default]
- pcre plugin loaded 394 rules.
- Monitoring /var/log/messages through pcre[default]
* WARNING: /var/log/everything/current does not exist.
prelude-client: error starting prelude-client: could not open '/etc/prelude/profile/prelude-lml/analyzerid' for reading

Profile 'prelude-lml' does not exist. In order to create it, please run:
prelude-adduser register prelude-lml "idmef:w" <manager address> --uid 0 --gid 0.
```

LML must be registered with uid and gid 0, since the process will be executed as root (to be able to analyze logs).

LML will then one for the One-Time Password(OTP), which will be provided by the manager:

```
Enter the one-shot password provided by the "prelude-adduser" program:
- enter registration one-shot password:
```

On the manager, run the following:

```
prelude-adduser registration-server prelude-manager
```

```
...
  - Starting registration server.
  - generated one-shot password is "dummypass".
  ...
```

Enter the password to the LML prompt:

```
  - enter registration one-shot password:
- confirm registration one-shot password:
- connecting to registration server (127.0.0.1:5553)...
- Anonymous authentication to registration-server successful.
- Sending certificate request.
```

The LML is now waiting for the Manager to sign the certificate.

On the manager, validate the certificate signing request:

```
- Anonymous authentication one-shot password check successful.
- Waiting for client certificate request.
- Analyzer with ID="3559090256170900" ask for registration with permission="idmef:w".
Approve registration [y/n]: y
The certificate is generated and sent to the client:
- Registering analyzer "3559090256170900" with permission "idmef:w".
- Generating signed certificate for client.
- Sending server certificate to client.
- ::ffff:127.0.0.1:47054 successfully registered.
```

On the client you will see:

```
LML registration is successful
- Receiving signed certificate.
- Receiving CA certificate.
- prelude-lml registration to 127.0.0.1 successful.
```

Now, the manager and the sensor have a trust relation, and can send messages to each other.This process takes some time, but it increases security and th communication between the sensor and the manager is encrypted.

Finally, the LML sensor should be up too:

```
/etc/init.d/prelude-lml start
```

```
Starting Prelude LML: prelude-lml.
  ps auxw | grep lml
  root      1946  0.3  0.0  20856  3424 ?        Ss   14:35   0:00 /usr/bin/prelude-lml -d -q -P /var/run/prelude-lml.pid
```

This concludes the first part.

Install Prewikka

Prewikka is the graphical frontend to Prelude, using a web server.

Installation

Prewikka requires two databases: one to get the Prelude alerts (which is the same as configured before), and one to store its own data (prewikka). Actually, the Ubuntu packages does only create the ***prewikka*** database, and does not configure access to Prelude alerts, so alert installation needs to be done manually.

Install Prewikka

```
apt-get install prewikka
```

The package will install required dependencies (python, for ex), and will ask for the database configuration. As for Prelude,we choose to use dbconfig-common, give the administrator password andpress enter for the DB password to let dbconfig-common generate one forus.

Configure Prelude-Manager Access

Get the password from prelude-manager configuration file ***/etc/prelude-manager/prelude-manager.conf*** and edit prewikka configuration file ***/etc/prewikka/prewikka.conf***:

```
vi /etc/prewikka/prewikka.conf
```

```
[idmef_database]
type: mysql
host: localhost
user: prelude
pass: **********
name: prelude
```

The [database] section is automatically configured by dbconfig-common, so do not modify it.

Web Server Configuration:

The configuration is explained in file ***/usr/share/doc/prewikka/README.Debian***. You can choose between 3 configurations:

- Apache / CGI setup with VirtualHost
- Apache / mod_python setup with VirtualHost
- Prewikka from the command line tool

As an example I'll use the ***mod_python*** setup.

```
apt-get install libapache2-mod-python
```

Add a VirtualServer to your apache configuration with the following content:

```
NameVirtualHost *
<VirtualHost *>
        ServerAdmin admin@domain.com
        <Location />
                SetHandler mod_python
                PythonHandler prewikka.ModPythonHandler
                PythonOption PrewikkaConfig /etc/prewikka/prewikka.conf
        </Location>

        <Location /prewikka>
                SetHandler None
        </Location>

        Alias /prewikka /usr/share/prewikka/htdocs
        Alias /htdocs /usr/share/prewikka/htdocs
</VirtualHost>
```

Restart you apache webserver and you can login to the prewikka interface.

Note: you can of course always us a setting for apache like:

```
NameVirtualHost xxx.xxx.xxx.xxx:80
<VirtualHost prewikka.yourdomain.tld:80>
```

This is usefull when you have other services running on your apache server.

Part 2: Installing And Configuring Snort

I will not write the complete howto for this since there is a hwto for snort: ***Intrusion Detection: Snort, Base, MySQL, and Apache2 On Ubuntu 7.10 (Gutsy Gibbon) (Updated)***.

I'll describe here the steps necessary to have ***snort*** logging to ***prelude***. In this setup you also don't need to install a ***mysql*** database and the base webinterface since ***snort*** will log to ***prelude*** and you can use the ***prewikka*** interface to see the ***snort*** alerts.

Follow all of the steps described in the howto above and replace the entry below with the new one:

Replace

```
./configure -enable-dynamicplugin --with-mysql

make
make install
```

With

```
./configure -enable-dynamicplugin --eanble-prelude

make
```

```
make install
```

Instead of doing:

Scroll down the list to the section with "# output database: log, mysql, user=", remove the "***#***" from in front of this line.
Change the "***user=root***" to "***user=snort"***, change the "***password=password***" to "***password=snort_password***", "***dbname=snort***"
Make note of the username, password, and dbname. You will need this information when we set up the Mysql db.
Save and quit.

Do:

Scroll down the list to the section with "# output alert_prelude: profile=snort", remove the "#Ã© in front of this line and that's it.

From step 5 on (***5. Set up the Mysql database.***) everything can be skipped.

Now we have to register the snort agent to the ***prelude manager***:

```
prelude-adduser register snort "idmef:w" <manager address> --uid snort --gid snort
```

On the ***prelude manager*** server:

```
prelude-adduser registration-server prelude-manager
```

This will register the snort agent to the prelude manager, as you did above for the prelude-lml.

Once the registration process is complete run:

```
snort -c /etc/snort/snort.conf
```

If everything goes right than you will see:

```
Initializing Network Interface eth0
Decoding Ethernet on interface eth0
- Connecting to 127.0.0.1:4690 prelude Manager server.
- TLS authentication succeed with Prelude Manager.
```

The entry eth0 depends on the ethernet adapter you specified. Important is that you see that snort is connecting to the prelude manager server and tls authentication was successfull.

If the agent is connecting, and you see ***snort*** in the agent list of ***prewikka*** than you can stop the process with ctrl-c and issue:

```
snort -c /snort/snort.conf -D
```

to start ***snort*** as a daemon. In the line above you can always add `-i ethX` if you don't listen on all network interfaces and want to specify a specific interface.

Part 3 : Installing And Configuring Ossec

First of all we will download and unpack the ***ossec source***:

```
cd /src
wget http://www.ossec.net/files/ossec-hids-1.4.tar.gz
tar xvzf ossec-hids-1.4.tar.gz
```

Now do the following to add ***prelude*** support:

```
cd ossec-hids-xx
cd src
make setprelude
```

Then edit ***Config.OS*** and add ***-lgcc_s*** in all lines ahead ***-lpthread*** like this:

```
CPRELUDE=-DPRELUDE -lprelude -pthread
-lgcc_s
```

 -L/usr/lib -lprelude -lgnutls -lgcrypt -lrt -ldl

The majority of this HOWTO is taken directly from the ***Installation Manual***for OSSEC-HID which is a very easy to follow manual. If you run intotrouble please look at the manual first as it will always have the mostup to date information.

Now the easy part. Ossec comes with an install script ***install.sh*** which does all of the hard work for us.

```
cd ..
./install.sh
```

Pick what language you want to read everything in and hit enter.

```
** Para instalaÃ§Ã£o em portuguÃªs, escolha [br].
  ** Fur eine deutsche Installation wohlen Sie [de].
  ** For installation in English, choose [en].
    ** Per l'installazione in Italiano, scegli [it].
  ** Aby instalowaÄ‡ w jÄ(TM)zyku Polskim, wybierz [pl].
  ** TÃ¼rkÃ§e kurulum iÃ§in seÃ§in [tr].
  (en/br/de/it/pl/tr) [en]:  en <enter>
```

Next it is going to warn us that we need a C compiler on themachine, and give yousome general information about your computer (kernel version, user and host).

 Go ahead and hit enter likes it says.

```
You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).
- System: Linux some information
- User: root
- Host: your hostname
-- Press ENTER to continue or Ctrl-C to abort. --
```

Next select a local install:

```
1- What kind of installation do you want (server, agent, local or help)? local <enter>
```

Now choose were you want to install it. Use the default or change it if you want to. This howto however will assume the default location.

```
Choose where to install the OSSEC HIDS [/var/ossec]:  <enter>
```

Now select you notification options. You can choose answers used in this howto ordifferent ones. I would recommend setting "Y" to everything. Active responses are really nice. It will set some default configurationvariables based on your answers and certian things it finds on yoursystem.

```
3- Configuring the OSSEC HIDS.

  3.1- Do you want e-mail notification? (y/n) [y]: y
```

- What's your e-mail address? ***youremail@yourdomain.com***
- What's your SMTP server ip/host? ***your smtp server address (localhost)***

3.2- Do you want to run the integrity check daemon? (y/n) [y]: ***y***

- Running syscheck (integrity check daemon).

3.3- Do you want to run the rootkit detection engine? (y/n) [y]: ***y***

- Running rootcheck (rootkit detection).

3.4- Active response allows you to execute a specific
command based on the events received. For example,
you can block an IP address or disable access for
a specific user.

```
       More information at:
       http://www.ossec.net/en/manual.html#active-response

   - Do you want to enable active response? (y/n) [y]: y

     - Active response enabled.

   - By default, we can enable the host-deny and the
     firewall-drop responses. The first one will add
     a host to the /etc/hosts.deny and the second one
     will block the host on iptables (if linux) or on
     ipfilter (if Solaris, FreeBSD or NetBSD).
   - They can be used to stop SSHD brute force scans,
     portscans and some other forms of attacks. You can
     also add them to block on snort events, for example.

   - Do you want to enable the firewall-drop response? (y/n) [y]: y

     - firewall-drop enabled (local) for levels >= 6

   - Default white list for the active response:
      - 192.168.2.1

   - Do you want to add more IPs to the white list? (y/n)? [n]: n

  3.6- Setting the configuration to analyze the following logs:
    -- /var/log/messages
    -- /var/log/auth.log
    -- /var/log/syslog
    -- /var/log/mail.info
    -- /var/log/apache2/error.log (apache log)
    -- /var/log/apache2/access.log (apache log)
```

```
 - If you want to monitor any other file, just change
   the ossec.conf and add a new localfile entry.
   Any questions about the configuration can be answered
   by visiting us online at http://www.ossec.net .



   --- Press ENTER to continue ---
```

Now it will compile everything. This shouldn't take too long tocomplete. It only took around 1-2 minutes for my box. After it iscompleted press enter to finish.

```
- Unknown system. No init script added.
- 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 maill it atossec-list@ossec.net(http://mailman.underlinux.com.br/mailman/listinfo/ossec-list).    More
information can be found at http://www.ossec.net
---  Press ENTER to finish (maybe more information below). ---
```

Now unfortunately it doesn't detect Ubuntu so it will not createan init script. This is simple enough to take care of. (Yes, its basic.If you want to improve it please feel free to do so) Copy and paste thefollowing into `/etc/init.d/ossec`:

```
#!/bin/sh

case "$1" in
start)
  /var/ossec/bin/ossec-control start
;;
stop)
  /var/ossec/bin/ossec-control stop
;;
```

```
restart)
  $0 stop && sleep 3
  $0 start
;;
reload)
  $0 stop
  $0 start
;;
*)
echo "Usage: $0 {start|stop|restart|reload}"
exit 1
esac
```

Now make it executable:

```
chmod +x /etc/init.d/ossec
```

Add it to our runlevels so it starts on boot:

```
update-rc.d ossec defaults
```

ossec.conf/var/ossec/etc/ossec.confossecprelude:

```
<global>
 ...
<prelude_output>yes</prelude_output>
</global>
```

Finally we'll add ***ossec*** as an agent in ***prelude***:

```
prelude-adduser registration-server prelude-manager
```

On the management server do:

```
prelude-adduser register OSSEC "idmef:w" localhost --uid ossec --gid ossec
```

Note: The sensor name MUST be in uppercase > OSSEC.

Start the ossec with init.d script powered by OSSEC (1.4 version should now detect ubuntu/debian OS and the init script will work!) or RShadow script.

If you see this you'r up and running.

```
Starting OSSEC HIDS v1.4 (by Daniel B. Cid)...
Connecting to 127.0.0.1:4690 prelude Manager server.
TLS authentication succeed with Prelude Manager.
```

Now go to the url where you installed ***prewikka***, and login with the user admin and password admin. Change this password immediately in order to prevent unauthorized access.