

---

# Intrusion Detection – 1.1

---

## **BUILDING AN IDS SOLUTION USING SNORT**

---

Aidan Carty  
Systems and Security Architect.  
Entropy Ltd.  
<http://www.entropy.ie>  
Email: [snort@entropy.ie](mailto:snort@entropy.ie)

## TABLE OF CONTENTS

---

1. Project Overview .....	4
1.1. OVERVIEW.....	4
1.2. WHAT IS SNORT ?.....	4
1.3. WHAT IS CARNOT+ ?.....	4
2. IDS Design .....	5
2.1. SOLUTION DESIGN. ....	5
NETWORK DIAGRAM .....	5
READ-ONLY INTERFACE CABLE.....	6
2.2. FURTHER READING. ....	6
3. Pre-Requisites .....	7
3.1. OVERVIEW.....	7
3.2. HARDWARE REQUIREMENTS.....	7
3.3. SOFTWARE REQUIREMENTS. ....	7
BASIC SOFTWARE.....	7
SOFTWARE USED FOR SNORT.....	8
4. Build Redhat .....	9
4.1. OVERVIEW.....	9
4.2. INSTALLATION OF REDHAT. ....	9
PARTITIONS - OVERVIEW .....	12
CREATE PARTITIONS.....	12
NETWORK CARD - ETH0.....	14
NETWORK CARD - ETH1 .....	15
CHANGE THE START-UP SCRIPTS. ....	19
HOSTS FILE.....	19
5. Building/Compiling .....	20
5.1. OVERVIEW.....	20
5.2. SETUP .....	20
EDITING OF CONFIGURATION FILES.....	20
5.3. COMPILING/INSTALLING – GDGRAPH.....	20
5.4. BUILD, INSTALL, CONFIGURE MYSQL.....	21
CONFIGURE MYSQL .....	22
USERNAME AND PASSWORD TABLE.....	22
SETUP THE SNORT DATABASES.....	22
5.5. BUILD/INSTALL OPENSSL.....	23
5.6. SETUP Mod_SSL .....	23
EXTRACT APACHE PACKAGE .....	23
5.7. BUILD, INSTALL, CONFIGURE APACHE. ....	23
SETUP OF AN X509 CERTIFICATE .....	23
CONFIGURE APACHE - DEFAULTS.....	24
CONFIGURE APACHE - EXTRAS.....	24
5.8. BUILD/INSTALL PHP4. ....	25
5.9. SETUP ACID AND DEPENDENCIES.....	25

<i>Entropy</i>	<i>Carnot+</i>
CREATE ACID TABLES.....	25
CONFIGURE ACID.....	26
5.10. SETUP OF FILE PERMISSIONS. ....	26
6. Snort.....	27
6.1. BUILDING SNORT.....	27
COMPILE LIBPCAP.....	27
BUILD SNORT 1.8.6 .....	27
6.2. CONFIGURE SNORT.....	27
DIRECTORIES.....	27
SETUP UP RULES.....	28
SETUP SNORT.CONF.....	28
QUICK TEST.....	28
6.3. ACID USAGE.....	29
7. Finish up.....	30
7.1. BOOT-UP CONFIGURATION SCRIPTS.....	30
START-UP OF MySQL.....	30
8. Hardening, Patching and security.....	31
8.1. OVERVIEW.....	31
8.2. SECURITY PATCHES. ....	31
8.3. BASTILLE.....	32
OVERVIEW.....	32
INSTALL.....	32
CONFIGURE.....	33
POST-INSTALL CHANGES.....	35
9. Appendix A .....	36
9.1. FURTHER REFERENCES.....	36
9.2. ENTROPY LTD. ....	36
9.3. DISCLAIMER. ....	36
9.4. NEW VERSIONS AND CHANGELOG. ....	37
CHANGELOG.....	37
TODO LIST FOR VER 1.2 .....	37
9.5. FEEDBACK. ....	37

## 1. PROJECT OVERVIEW

---

### 1.1. Overview.

This document provides a step-by-step guide to building an intrusion detection system using open-source software, the process involves.

- ◆ Installing RedHat Linux 7.1
- ◆ Compiling/Installing and configuration of MySql/Apache/ACID/Snort
- ◆ Setup of Snort rules
- ◆ Hardening of Machine

The document assumes a basic level understanding of linux and computer technologies.

### 1.2. What is snort ?.

<http://www.snort.org/about.html>

Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks.

It can perform protocol analysis and content searching/matching in order to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture.

Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, user specified files, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient.

Plug-ins allow the detection and reporting subsystems to be extended. Available plug-ins include database or XML logging, small fragment detection, portscan detection, and HTTP URI normalization, IP defragmentation, TCP stream reassembly and statistical anomaly detection.

### 1.3. What is Carnot+ ?.

Carnot+ is a methodology used by Entropy Ltd for the delivery of professional services, the methodology is used throughout the organisation from the R&D team, Sales team, Logistics, Engineering, Service Desk and Marketing.

This document is a summary of some of the information available to and designed by the different groups as per the Carnot+ process.

The full Carnot+ process is outside the scope of this document.

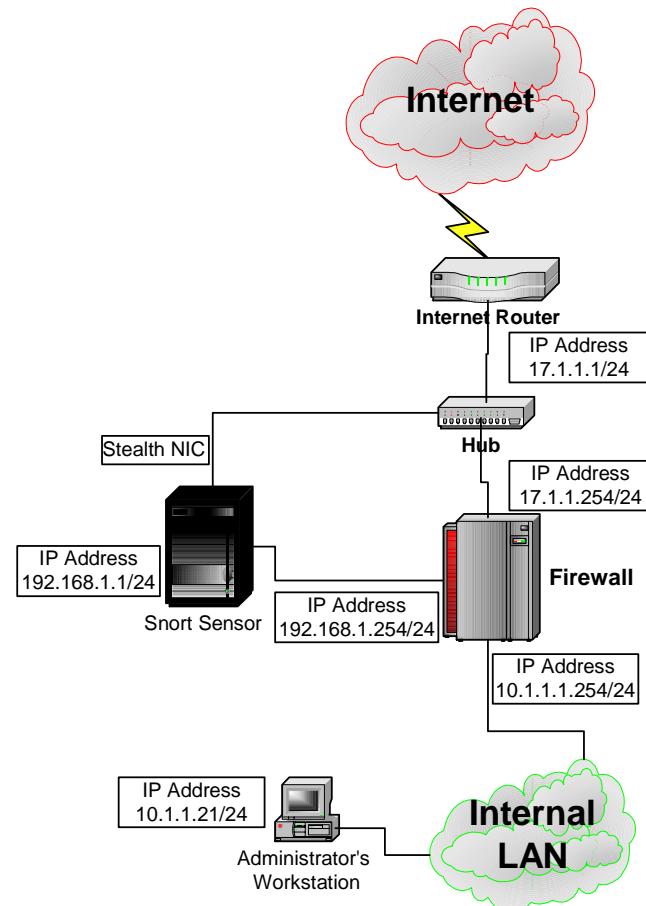
## 2. IDS DESIGN

### 2.1. Solution Design.

The following diagram shows a simple example of where to place a snort sensor. We will be using the information in the below network diagram during the configuration of our snort sensor.

In this example internet bound traffic i.e. web and email travels from the internal lan through the firewall out through the internet router and out to the respective destinations, inbound traffic passes back in the same way.

Network Diagram



The key points are

- ◆ The snort sensor is placed in a key position to monitor all internet based traffic in and out of the organisation.
- ◆ The firewall adds an extra layer of security to the solution, by placing the snort sensor in a dmz connected to the firewall

The snort sensor machine has 2 network cards.

- ◆ The first interface (eth0) of the snort box is linked to an interface off the firewall, the firewall is configured to only allow the Administrators pc connect to the snort sensor for https and ssh services, all other traffic to and from the snort machine is silently dropped by the firewall.
- ◆ The second interface (eth1) watches all of the traffic passing between the firewall and the internet router. The network card is configured with no ip address and in our example were using a hub, if your using a switch then a mirror/span port needs to be setup and the snort sensor plugged into it. (See the relevant switch manuals)

### Read-Only Interface Cable

See the following link on instructions to create a Read-only ethernet cable, used to connect the hub/switch to the second nic of the snort sensor. <http://www.silicondefense.com/techsupport/ro-ethernet.htm>

## 2.2. Further Reading.

The full complexities of network intrusion detection design are outside the scope of this document but the following book and document are recommended.

- ◆ Northcutt, Stephen and Novak, Judy and McLachlan, Donald. Network Intrusion Detection Second Edition. Indianapolis: New Riders Publishing, 2001.
- ◆ Deployment of IDS in complex network environments.  
<http://www.snort.org/docs/iss-placement.pdf>

## 3. PRE-REQUISITES

---

### 3.1. Overview.

Before you begin make sure you have all of the below hardware requirements.

### 3.2. Hardware Requirements.

For this build, the server must have at least the following minimum specification.

- ◆ Pentium III 500mhz
- ◆ 128 MB of RAM
- ◆ 4 Gig Hard Disk or greater
- ◆ 2 PCI-based Network Interface Cards

All hardware must also be on the redhat hardware compatibility list.

<http://hardware.redhat.com/hcl/>

### 3.3. Software Requirements.

This document uses particular versions of software, newer versions are generally available but the following versions have been tested so that they will work together.

#### Basic Software

Redhat 7.1 – Binary cd-1 and Binary cd-2 – <http://www.redhat.com>  
Operating system for console and sensors.

Windows SSH Client, if the administrative workstation is windows based then the following client software is necessary, as by default OpenSSH is enabled on Redhat 7.1

- ◆ TTSSH is a free SSH client for Windows.  
<http://www.zip.com.au/~roca/ttssh.html>

Installation of this product is outside the scope of this document.

### Software used for Snort

Before starting, put the binaries on cdrom or make them available on an ftp server.

mysql-3.23.42 - <http://www.mysql.com/>  
Database to store alerts.

apache\_1.3.23 - <http://www.apache.org>  
Web server that will run the console and reporting software.

openssl-0.9.6c - <http://www.openssl.org>  
Library that performs encryption/decryption for mod\_ssl.

mod\_ssl-2.8.7-1.3.23 - <http://www.modssl.org>  
Enables Apache to provide SSL-secured web pages.

Acid-0.9.6b21 - <http://www.cert.org/kb/acid>  
Analysis Console Engine for Intrusion Detection, a PHP-based analysis engine to search and process the data generated by the Snort sensor.

php-4.1.2 – <http://www.php.net>  
PHP is a web based general-purpose scripting language, used by ACID.

adodb172 - <http://phplens.com/lens/dl>  
This is database abstraction library used by ACID.

gd-1.8.4 - <http://www.boutell.com/gd>  
A graphics library for fast image creation.

phplot-4.4.6 - <http://www.sourceforge.net/phplot/>  
This routine is a class for creating scientific and business charts.

snort-1.8.6 - <http://www.snort.org/dl/>  
Intrusion Detection software for the sensors, the core of the system.

snort-rules-current. - <http://www.snort.org/dl/signatures/>  
The latest snort rules.

Libpcap version 0.7.1- <http://www.tcpdump.org/>  
Library that handles the actual capturing of packets from the network interface.

bastille 1.3.0-1.0 - <http://bastille-linux.sourceforge.net/>  
Security hardening script for the Redhat Linux Operating System.

## 4. BUILD REDHAT

---

### 4.1. Overview.

Let's start.

The below url provides a good reference guide to installing RH-Linux 7.1,  
<http://www.redhat.com/docs/manuals/linux/RHL-7.1-Manual/install-guide>

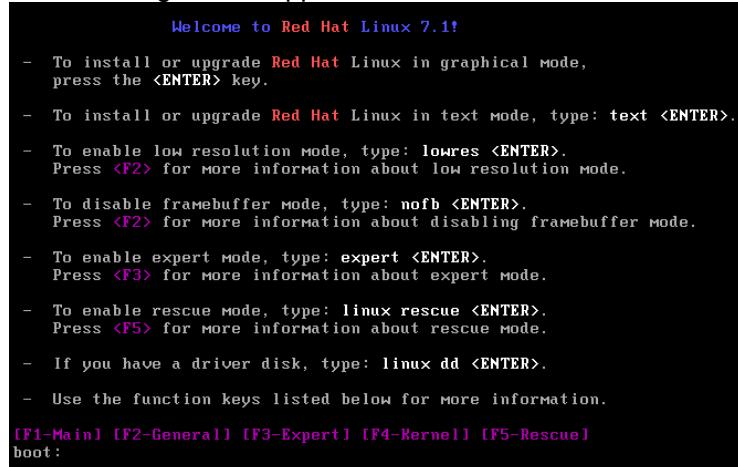
The following screenshots are based on this document.

### 4.2. Installation of Redhat.

Unpack the server, install the network cards, plug everything in, turn on the machine (You may need to change a BIOS setting to allow boot of cdrom).

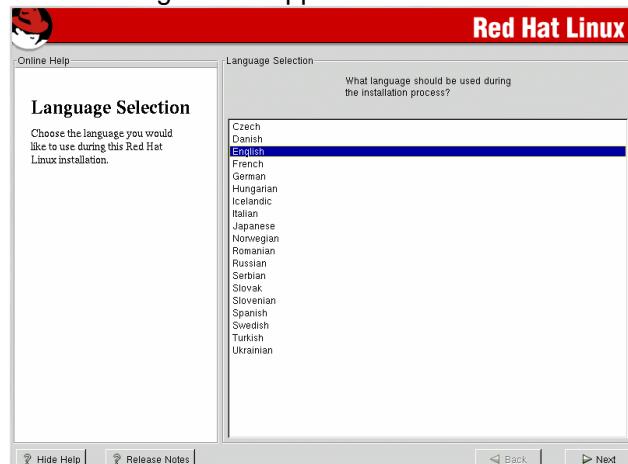
Insert Redhat CD-Rom1 and boot away.

The following screen appears.



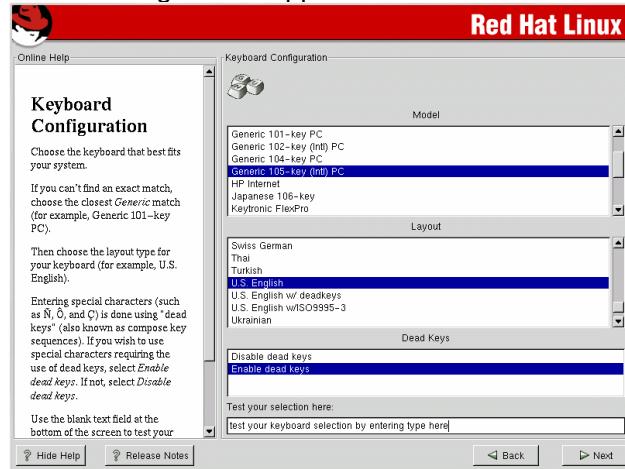
Hit Enter

The following screen appears



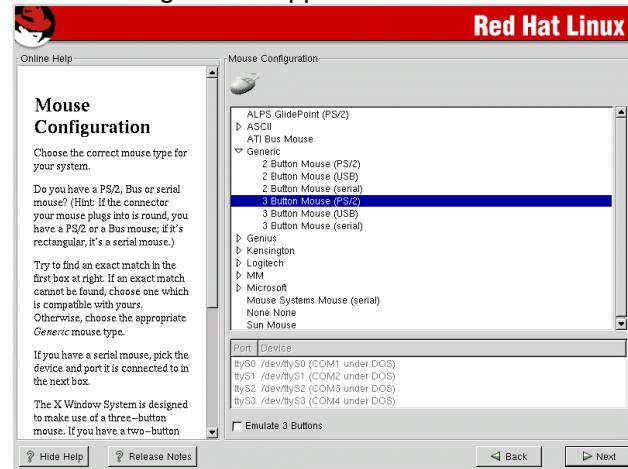
Choose English, Click Next.

The following screen appears



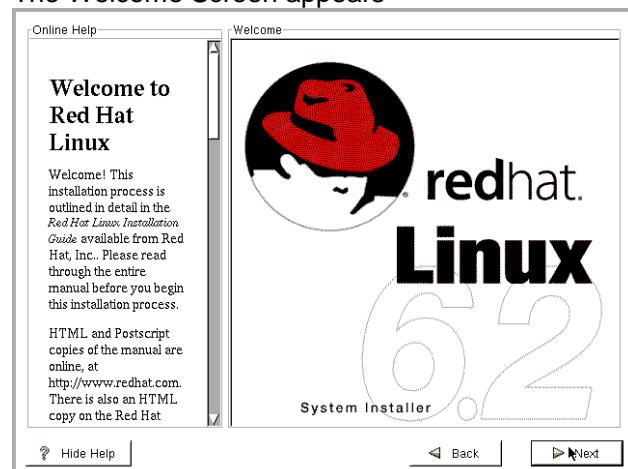
set the Layout to be "United Kingdom"  
Click Next.

The following screen appears



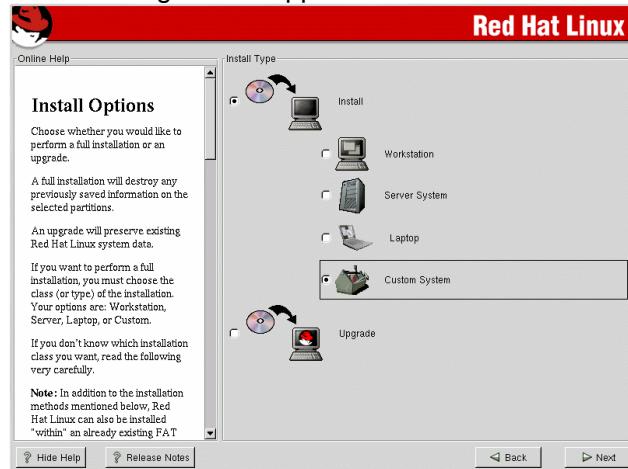
Set mouse to be "2 button (PS2)" -  
(This is dependant on your mouse hardware)  
Click Next

The Welcome Screen appears



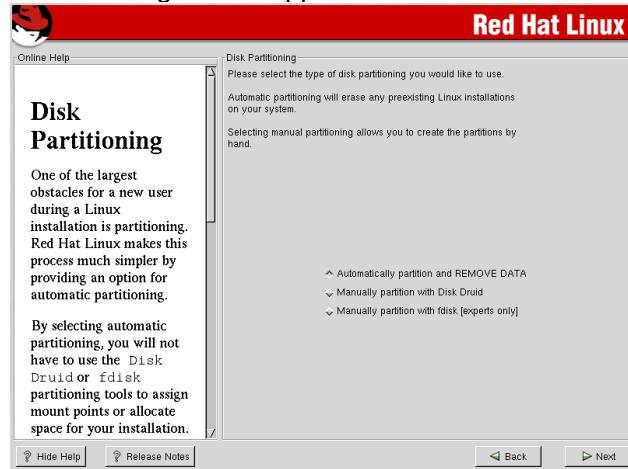
Click on Next

The following screen appears



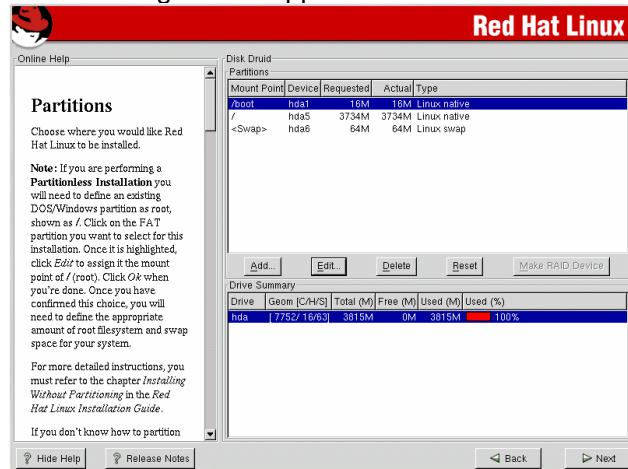
Click on the item "Custom System"  
Click on Next

The following screen appears



Click on "Manually partition with Disk Druid"  
Click Next.

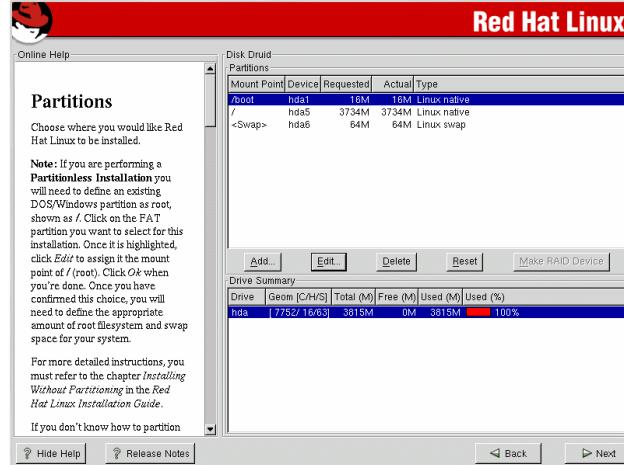
The following screen appears



## Partitions - Overview

Depending on the previous use of the machine e.g. Windows NT etc. You will need to delete all the existing partitions.

To delete, highlight a partition, click on the Delete button, Click Yes.



Now create the following partitions, we have a 14GB disk, so the breakdown would be as follows.

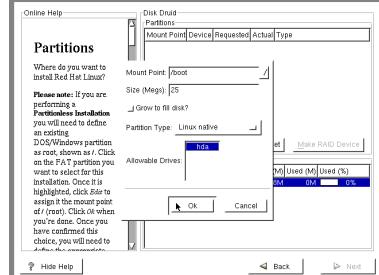
/boot - 31MB  
 / - 1027MB - root partition  
 /usr - 1027MB - snort/acid/apache/mysql binaries.  
 <swap> - 258MB - swap partition  
 /var - 11976MB - log and database storage.

(Our linux installation size will be around 500MB, using the above partition strategy and after installation /boot = 3.5MB, / = 54MB, /usr=362MB, /var=7.8MB. If you have a larger or smaller disk, then use the above partition strategy as a guideline, the /var partition is created last and enabled with the “Use remaining space” option, see below. )

## Create Partitions

To create a standard “Linux Native” Partitions, click on the ADD button.

The following screen appears.

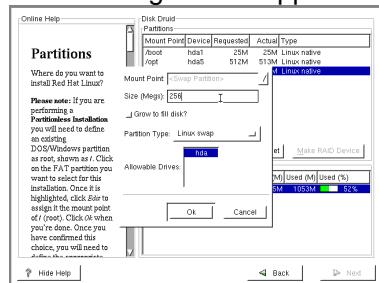


In the above example we are creating a /boot partition.

- ◆ Enter the mount point as /boot
- ◆ Enter the Size = 31MB
- ◆ Partition Type “Linux Native”

Click OK

To create a swap file, which is necessary and usually around twice the size of available physical ram, click on the ADD button  
 The following screen appears

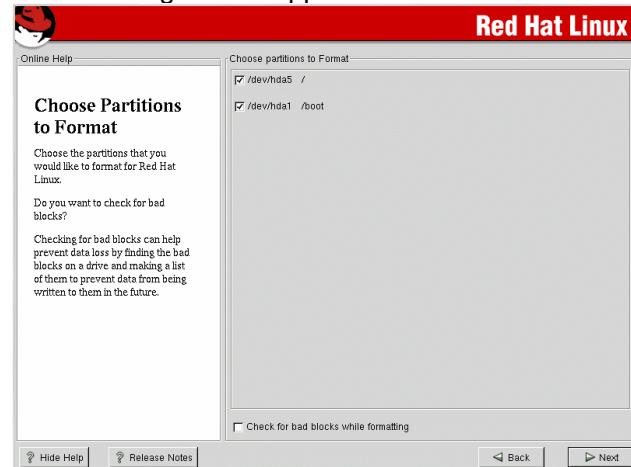


- ◆ Change the Partition Type to “Linux Swap”
- ◆ Enter the Size = 256MB (2\*128MB)

Click OK

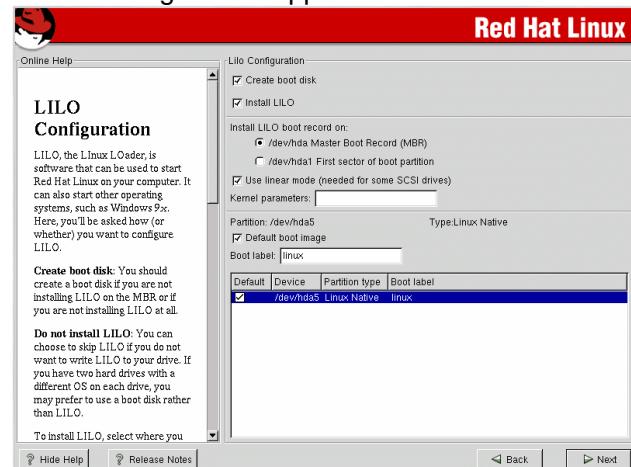
When all of the above partitions have been created click Next

The following screen appears.



Accept the defaults, Click Next.

The following screen appears.

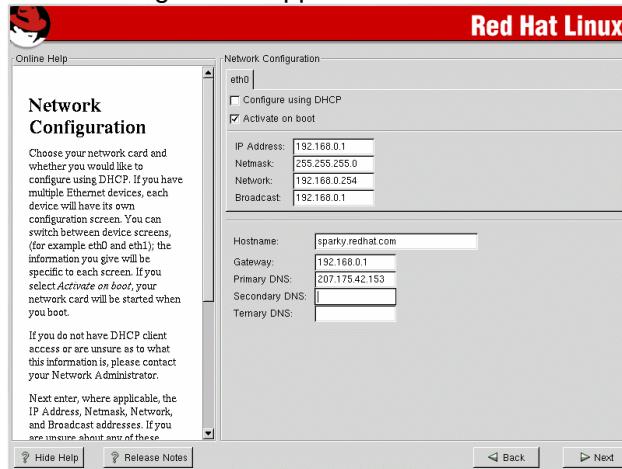


Untick “Create boot disk” (This will be created at a later stage)

Accept the defaults.

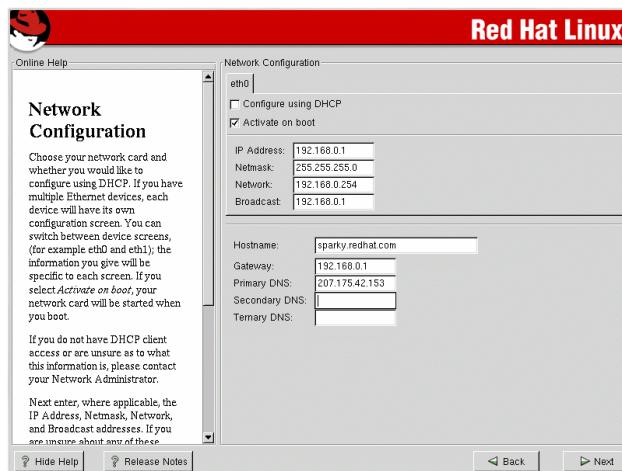
Click Next

The following screen appears



The snort sensor has 2 network cards. (referenced as eth0 and eth1)

Network card - eth0



Untick "Configure using DHCP" on the Tab – eth0

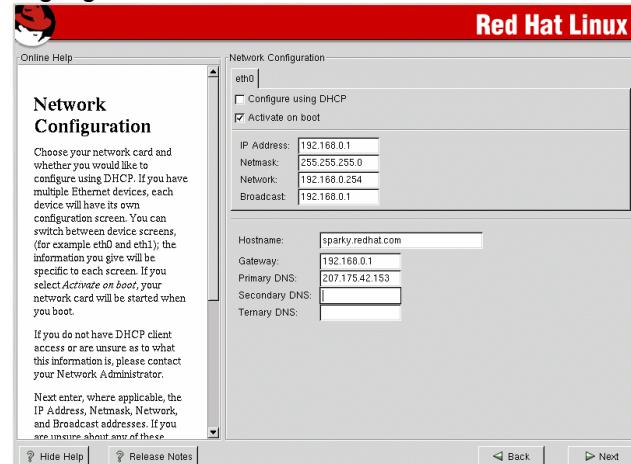
Enter the following information as per the above network diagram.  
(or use your own information)

Heading	Value
IP Address	192.168.1.1
Netmask	255.255.255.0
Network	192.168.1.0
Broadcast	192.168.1.255
Hostname	entropy-snort
Gateway	192.168.1.254
Primary DNS	N/A - (Don't have one in our example)
Secondary DNS	"
Tertiary	"

Click on the Tab eth1

## Network card - eth1

Highlight the second Tab – eth1

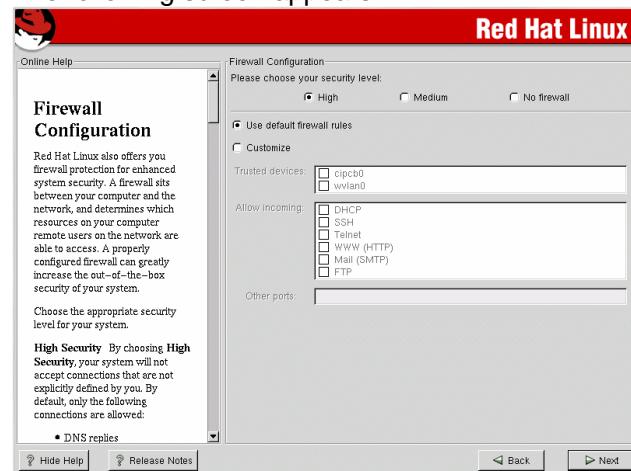


Untick "Configure using DHCP" on the Tab – eth1

Untick "Activate on boot"

Click Next

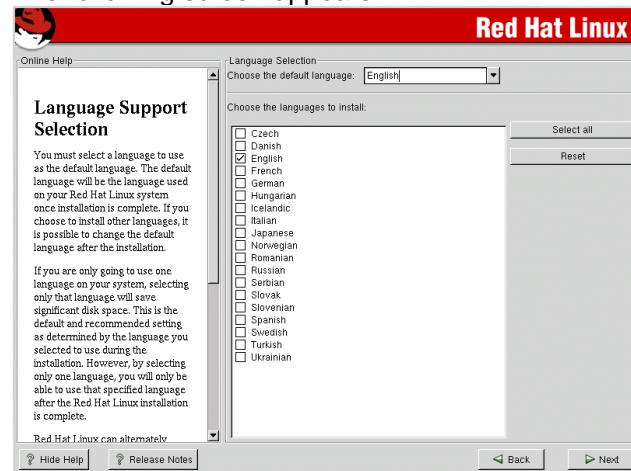
The following screen appears



Click on "No firewall"

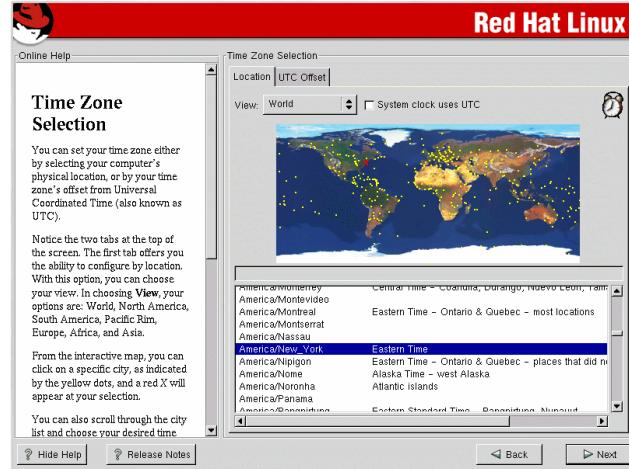
Click Next

The following screen appears



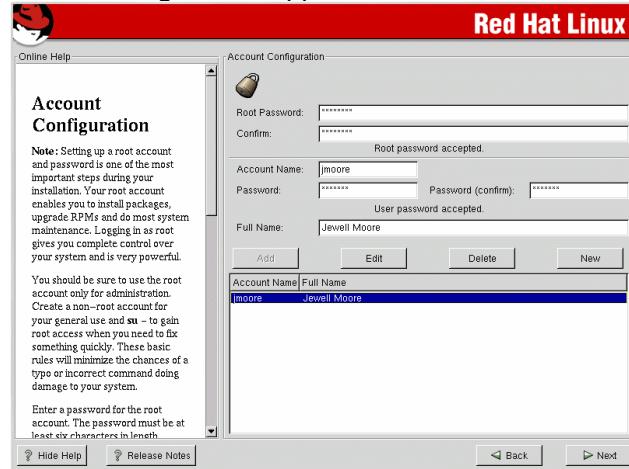
Untick – English (USA)  
 Tick - English (Ireland).  
 Click Next

The following screen appears



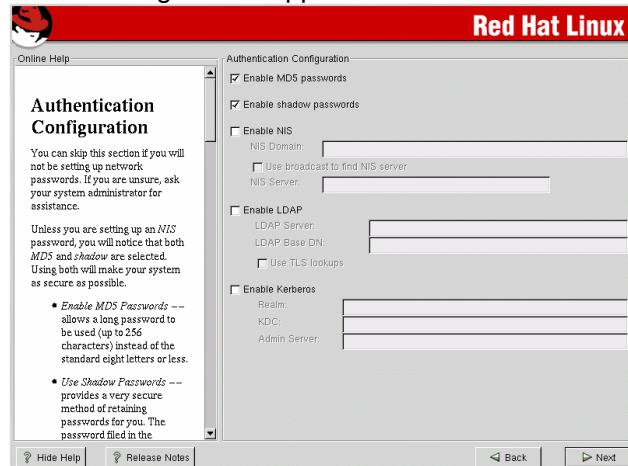
Change the “View” to Europe  
 Setup as “Europe/Dublin”  
 Click Next

The following screen appears



Enter the root password and again to confirm.  
 Click Next

The following screen appears



Accept the defaults and Click Next

The following screen appears

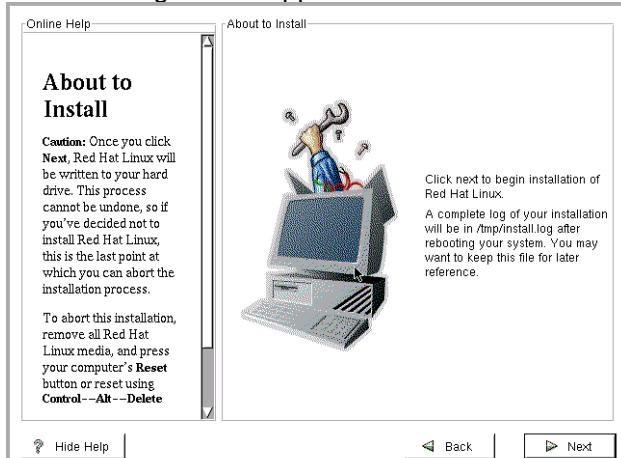


Disable all of the Package groups except the following.

- ◆ Networked Workstation
- ◆ Network Management Workstation
- ◆ Development.
- ◆ Utilities

Click Next

The following screen appears



Click Next

The following screen appears



The partitions are created/formatted and the packages are installed, all errors are put into /tmp/install.log

When prompted put in CD-ROM2, click OK.

Installation continues.

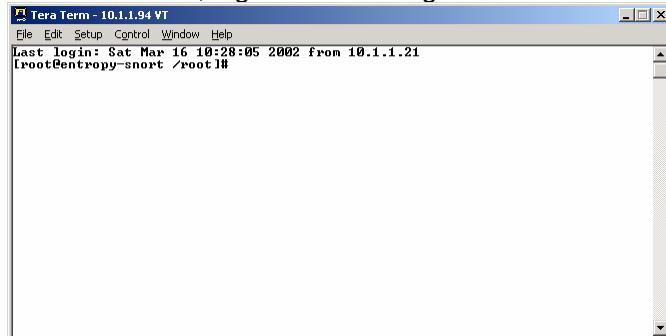
The final screen appears



Click Exit

The Server ejects the cdrom and reboots

After the reboot, login as root using the ssh client.



### Change the Start-up Scripts.

Run the following commands, to reduce the number of services loaded during boot up of the server.

- ◆ cd /etc
- ◆ mv /etc/rc2.d /etc/rc2.d\_bak
- ◆ mv /etc/rc3.d /etc/rc3.d\_bak
- ◆ mkdir /etc/rc2.d
- ◆ mkdir /etc/rc3.d
- ◆ ln -s ..../init.d/sshd /etc/rc3.d/S55sshd && ln -s ..../init.d/network /etc/rc3.d/S10network && ln -s ..../init.d/syslog /etc/rc3.d/S12syslog && ln -s ..../init.d/crond /etc/rc3.d/S90crond && ln -s ..../init.d/random /etc/rc3.d/S20random && ln -s ..../rc.local /etc/rc3.d/S99local
- ◆ Reboot the server

### Hosts file

A hosts entry for the snort server needs to be put into the hosts file, run the following commands (see the reference for use of the vi editor in the next section)

- ◆ cd /etc
- ◆ vi hosts
- ◆ Add the following line, without quotes below the “127.0.0.1” text.  
“192.168.1.1 entropy-snort entropy-snort.entropy.ie”
- ◆ Save and exit

## 5. BUILDING/COMPILED

### 5.1. Overview.

Now that linux has been installed we are going to compile the binaries.

The files used need to be copied onto our new server, from an existing ftp server or from a cdrom.

### 5.2. Setup.

Login into the server and create a directory for the files, using the following command

- ◆ mkdir /usr/local/acid\_setup\_files

copy all the files into this directory from a cdrom or from an ftp server.

```
[root@Entropy-snort acid_setup_files]# ls -la
total 23812
drwxr-xr-x  2 root  root   4896 Mar 16 10:36 .
drwxr-xr-x 12 root  root  4896 Mar 16 10:35 ..
-rw-r--r--  1 root  root 109706 Mar 16 10:35 acid-0.9.6b20.tar.gz
-rw-r--r--  1 root  root 172735 Mar 16 10:35 adodb172.tgz
-rw-r--r--  1 root  root 224100 Mar 16 10:35 Bastille-1.2.0-1.3.23.tar.gz
-rw-r--r--  1 root  root 137586 Mar 16 10:36 Bastille-1.2.0-1.lmdk.no
arch.rpm
-rw-r--r--  1 root  root  24323 Mar 16 10:36 Bastille-Curses-module-1.2.0-1.lmdk.no
-rw-r--r--  1 root  root 257631 Mar 16 10:35 gd-1.8.4.tar.gz
-rw-r--r--  1 root  root 197653 Mar 16 10:35 libpcap-0.7.1.tar.gz
-rw-r--r--  1 root  root 751993 Mar 16 10:35 mod_ssl-2.8.7-1.3.23.tar.gz
...
-rw-r--r--  1 root  root 11769768 Mar 16 10:35 mysql-3.23.42.tar.gz
-rw-r--r--  1 root  root 2151178 Mar 16 10:35 openssl-0.9.6e.tar.gz
-rw-r--r--  1 root  root  59898 Mar 16 10:36 perl-Curses-1.05-2mdk.15
RPM
-rw-r--r--  1 root  root  335964 Mar 16 10:35 php-4.1.2.tar.gz
-rw-r--r--  1 root  root  98085 Mar 16 10:35 phplot-4.4.6.tar.gz
-rw-r--r--  1 root  root 172068 Mar 16 10:35 snort-1.8.3.tar.gz
-rw-r--r--  1 root  root 376086 Mar 16 10:35 snortdb-extra.gz
-rw-r--r--  1 root  root  67596 Mar 16 10:35 snortrules.tar.gz
[root@Entropy-snort acid_setup_files]#
```

### Editing of configuration files

Throughout the use of this document, we will be using the vi editor to edit files, see the following link, which has a tutorial on the vi editor.

<http://www.linux.ie/articles/tutorials/vi.php>

### 5.3. Compiling/Installing – GdGraph.

To compile and install the gd-graph package run the following commands.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ tar -zvxf gd\*
- ◆ cd gd\*
- ◆ mkdir /usr/local/include
- ◆ make && make install

## 5.4. Build, Install, Configure MySQL.

To compile and install the MySQL package run the following commands.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ tar -zxvf mysql-3.23.42.tar.gz
- ◆ cd mysql-3.23.42
- ◆ ./configure --prefix=/usr/local/mysql --localstatedir=/var/mysql
- ◆ make && make install

After compilation and installation, run the following

- ◆ scripts/mysql\_install\_db
- ◆ echo /usr/local/mysql/lib/mysql >> /etc/ld.so.conf && ldconfig
- ◆ groupadd mysql
- ◆ useradd -g mysql mysql
- ◆ chown -R root:mysql /usr/local/mysql
- ◆ chown -R mysql /usr/local/mysql/bin
- ◆ chown -R mysql /var/mysql
- ◆ scripts/mysql\_install\_db

Run the following commands, make a note of the MySQL root password used, in our example its entropy1, VERY important that the password is surrounded by single quotes.

- ◆ cd /usr/local/mysql
- ◆ bin/safe\_mysqld --user=mysql &
- ◆ bin/mysqladmin -u root password 'entropy1'

Edit the file /etc/profile using vi and put the following text before the line in the /etc/profile file and run the source command.

- ◆ vi /etc/profile  
Navigate to above the following line.  
"export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE  
INPUTRC"
- ◆ Add the following line  
PATH=\$PATH:/usr/local/mysql/bin:/usr/local/apache/bin
- ◆ Save and exit vi
- ◆ Run the following command  
source /etc/profile

## Configure MySQL

Run the following commands to setup the MySQL tables.

- ◆ mysqladmin -u root -p drop test  
(Enter the MySQL-root password configured in the last section i.e. entropy1 and then confirm with y to delete)
- ◆ mysql -p  
(Enter the MySQL-root password configured in the last section i.e. entropy1)
- ◆ \u mysql
- ◆ DELETE FROM user WHERE User="";  
(Must be 2 single quotes)
- ◆ DELETE FROM user WHERE Password="";  
(Must be 2 single quotes)
- ◆ GRANT ALL PRIVILEGES ON \*.\* TO dba@localhost IDENTIFIED BY 'entropy1\_dba';  
(Make a note of the password used, in our example its entropy1\_dba, VERY important that the password is surrounded by single quotes.)
- ◆ CREATE DATABASE snort;
- ◆ GRANT INSERT,SELECT,DELETE,UPDATE ON snort.\* to  
snort@localhost IDENTIFIED BY 'entropy1\_snort';  
(Make a note of the snort password used, in our example its entropy1\_snort, VERY important that the password is surrounded by single quotes.)
- ◆ Type “exit” - no quotes

### Username and password table

Username	Password
root (MySQL root)	entropy1
dba	entropy1_dba
snort	entropy1_snort

### Setup the snort databases.

The snort files need to be extracted and the snort database tables need to be created. The above dba password will be prompted for during the setup.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ tar -zvxf snort-1.8.6.tar.gz
- ◆ mysql -u dba -p snort < snort-1.8.6/contrib/create\_mysql  
(Using the dba password - entropy1\_dba)
- ◆ zcat snort-1.8.6/contrib/snortdb-extra.gz | mysql -u dba -p snort  
(Using the dba password - entropy1\_dba)

## 5.5. Build/Install OpenSSL.

To compile and install the OpenSSL package run the following commands.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ tar -zvxf openssl-0.9.6c.tar.gz
- ◆ cd openssl-0.9.6c
- ◆ sh config \ no-idea \ no-threads \ -fPIC && make && make install

## 5.6. Setup Mod\_SSL.

### Extract Apache package

Before setup of the Mod\_SSL libraries, the apache files need to be extracted.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ tar -zvxf apache\_1.3.23.tar.gz

Now setup mod\_ssl

- ◆ cd /usr/local/acid\_setup\_files
- ◆ tar -zvxf mod\_ssl-2.8.7-1.3.23.tar.gz
- ◆ cd mod\_ssl-2.8.7-1.3.23
- ◆ ./configure --with-apache=../apache\_1.3.23/ --with-ssl=../openssl-0.9.6c/ --prefix=/usr/local/apache --enable-shared=ssl --enable-module=ssl --enable-rule=SSL\_SDBM --enable-rule=SSL\_EXPERIMENTAL --enable-rule=SSL\_VENDOR --enable-rule=EAPI

(If you're going to use a later version of apache or openssl, change the directory as appropriate in the above section i.e. “./apache\_1.3.23” or “./openssl-0.9.6c”) - When pasting the above bit make sure it's formatted for one line and spaces between the options e.g. “--enable-rule”

## 5.7. Build, Install, Configure Apache.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ cd apache\_1.3.23
- ◆ make && make certificate && make install

### Setup of an X509 Certificate

During the installation a self signing X509 certificate needs to be created as we are going to be using a https connection for ACID.

During the install the following options are setup

Step 0 - Signature Algorithm ((R)SA or (D)SA) [R]:  
Choose R

Step 1 - Generating RSA private key (1024 bit) [server.key]

Step 2 – Generating X509, fill in the following details or use your own.

Heading	Values
Country Name	IE
State or Province Name	Dublin
Locality Name	Sandyford
Organization Name	Entropy Ltd
Organizational Unit Name	Carnot+
Common Name	entropy-snort
Email Address	bobthebuilder@ie
Certificate	365

Step 3 - Certificate Version (1 or 3) [3]:

Choose 3

Step 4 – Encrypt the private key now? [Y/n]:

Choose n

### Configure Apache - Defaults

First remove the default directories

- ◆ cd /usr/local/apache
- ◆ mv htdocs htdocs\_old
- ◆ mkdir htdocs

Change the http.conf files

- ◆ cd /usr/local/apache/conf
- ◆ vi httpd.conf

Configure the following settings

Setting	Value
MinSpareServers	1
MaxSpareServers	3
StartServers	2
MaxClients	5
Port	443
ServerSignature	off

- ◆ Save and Exit httpd.conf

### Configure Apache - Extras

- ◆ cd /usr/local/apache/conf
- ◆ vi httpd.conf
- ◆ Navigate to the section.  
<IfDefine SSL>  
Listen 80,  
Listen 443  
</IfDefine>
- ◆ Put a # in front of “Listen 80”
- ◆ Save and exit

## 5.8. Build/Install PHP4.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ tar -zxvf php-4.1.2.tar.gz
- ◆ cd php-4.1.2
- ◆ ./configure --with-mysql=/usr/local/mysql --with-apxs=/usr/local/apache/bin/apxs --enable-bcmath --with-gd --enable-sockets --enable-track-vars && make && make install && cp php.ini-dist /usr/local/lib/php.ini
- ◆ vi /usr/local/apache/conf/httpd.conf
- ◆ Navigate to after the line "AddType application/x-tar .tgz"
- ◆ Add the following lines.  
AddType application/x-httdp-php .php  
AddType application/x-httdp-php-source .phps
- ◆ Save and exit

## 5.9. Setup ACID and Dependencies.

The following files need to be extracted and then copied into the apache directory

- ◆ cd /usr/local/acid\_setup\_files
- ◆ tar -zxvf acid\*
- ◆ mv acid /usr/local/apache/htdocs/acid
- ◆ tar -zxvf adodb\*
- ◆ mv adodb /usr/local/apache/htdocs/adodb
- ◆ tar -zxvf phplot\*
- ◆ mv phplot-4.4.6 /usr/local/apache/htdocs/phplot

### Create ACID tables

Run the following command to create the Acid database tables.

- ◆ mysql -u dba -p snort < /usr/local/apache/htdocs/acid/create\_acid\_tbls\_mysql.sql  
(Using the dba password - entropy1\_dba)

### Configure ACID

- ◆ cd /usr/local/apache/htdocs/acid/
- ◆ vi /usr/local/apache/htdocs/acid/acid\_conf.php
- ◆ Make the following changes.

Setting
\$Dblib_path="/usr/local/apache/htdocs/adodb";
\$alert_dbname: "snort";
\$alert_host: "localhost";
\$alert_port: "3306";
\$alert_user: "snort";
\$alert_password: "entropy1_snort";
(See the password table from the previous MySQL section)
\$ChartLib_path="/usr/local/apache/htdocs/phplot";

- ◆ Save and exit

### 5.10. Setup of file permissions.

Set the following permissions.

- ◆ chmod 0755 /usr/local/apache/htdocs/acid
- ◆ chmod 0644 /usr/local/apache/htdocs/acid/\*
- ◆ chmod 0755 /usr/local/apache/htdocs/adodb
- ◆ chmod 0644 /usr/local/apache/htdocs/adodb/\*
- ◆ chmod 0755 /usr/local/apache/htdocs/phplot
- ◆ chmod 0644 /usr/local/apache/htdocs/phplot/\*
  
- ◆ chown -R root:wheel /usr/local/apache/htdocs/acid/\*
- ◆ chown -R root:wheel /usr/local/apache/htdocs/adodb/\*
- ◆ chown -R root:wheel /usr/local/apache/htdocs/phplot/\*

## 6. SNORT

---

### 6.1. Building Snort.

#### Compile libpcap

The libpcap libraries need to be compiled before installing snort.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ tar -zxvf libpcap-0.7.1.tar.gz
- ◆ cd libpcap-0.7.1
- ◆ ./configure && make && make install

#### Build Snort 1.8.6

- ◆ cd /usr/local/acid\_setup\_files
- ◆ cd snort-1.8.6 (the files were extracted earlier)
- ◆ ./configure --with-mysql=/usr/local/mysql --with-openssl=/usr/local/ssl && make && make install
- ◆ snort -v (quick test)

### 6.2. Configure Snort.

#### Directories

We are going to create directories for the logs and snort rules.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ mkdir /var/snort\_log\_storage
- ◆ mkdir /usr/local/snort
- ◆ mv /usr/local/bin/snort /usr/local/snort
  
- ◆ groupadd snort
- ◆ useradd -g snort snort
- ◆ passwd -l snort
- ◆ chmod 700 -R /usr/local/snort
- ◆ chown -R snort.snort /usr/local/snort
- ◆ chmod 700 -R /var/snort\_log\_storage
- ◆ chown -R snort.snort /var/snort\_log\_storage

### Setup up rules

We are going to extract the snort rules to the newly created directory.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ tar -zxvf snortrules.tar.gz
- ◆ mv rules /usr/local/snort
- ◆ chmod 700 -R /usr/local/snort/rules
- ◆ chown -R snort.snort /usr/local/snort/rules

### Setup snort.conf

We are going to make changes to the snort configuration file (snort.conf)

- ◆ cd /usr/local/snort/rules
  - ◆ vi /usr/local/snort/rules/snort.conf
- Change following variables.

Value
var HOME_NET 17.1.1.0/24 (using the network diagram from the IDS design section)
preprocessor portscan: \$HOME_NET 4 3 /var/snort_log_storage/portscan.log (Change the logfile of the above portscan preprocessor)
output database: log, mysql, user=snort password=entropy1_snort dbname=snort host=localhost

- ◆ Save and Exit

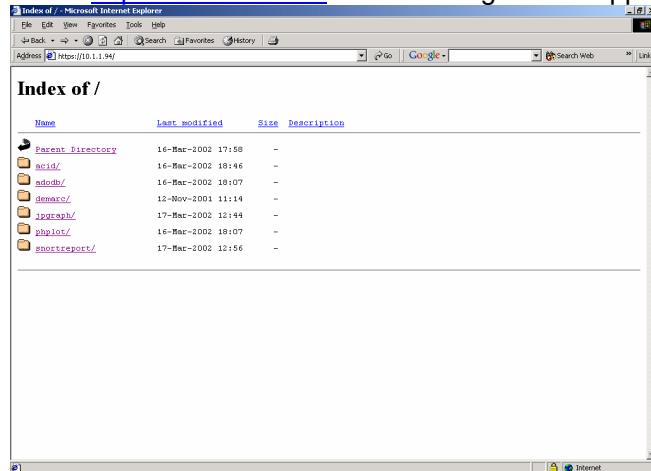
### Quick Test

As a quick test, run the following commands...

- ◆ ifconfig eth1 up  
(Bring up the second interface)
- ◆ /usr/local/mysql/bin/safe\_mysqld --user=mysql &  
(Start-up MySql)
- ◆ /usr/local/apache/bin/apachectl startssl  
(Start-up Apache)
- ◆ /usr/local/snort/snort -i eth1 -c /usr/local/snort/rules/snort.conf -u snort  
-g snort -b -l /var/snort\_log\_storage &  
(Start-up Snort)

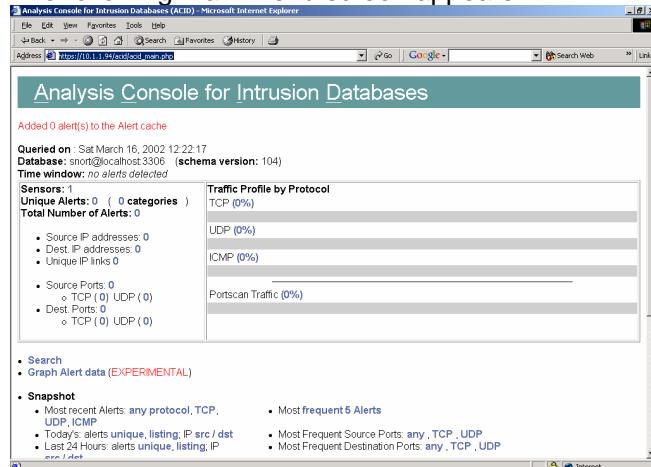
### 6.3. Acid Usage.

After startup, open your browser and enter the following URL - <https://192.168.1.1/> The following screen appears



Click on the ACID directory.

The following main menu screen appears



See the ACID homepage for usage instructions.

<http://www.cert.org/kb/acid/>

## 7. FINISH UP

---

### 7.1. Boot-up configuration scripts.

You will want to make some entries in the rc.local file to start up MySQL, Apache and Snort on boot-up.

#### Start-up of MySql

- ◆ vi /etc/rc.local
- ◆ Navigate to the bottom of the rc.local and enter the following text.

```
echo "Starting up MySql."
/usr/local/mysql/bin/safe_mysqld --user=mysql &
echo "Starting up Apache."
/usr/local/apache/bin/apachectl startssl
echo "Starting up Snort."
/usr/sbin/ifconfig eth1 up
/usr/local/snort/snort -i eth1 -c /usr/local/snort/rules/snort.conf -u snort
-g snort -b -l /var/snort_log_storage &
```
- ◆ Save and Exit vi
- ◆ Reboot the server

## 8. HARDENING, PATCHING AND SECURITY

### 8.1. Overview.

In this document we provide security for our snort machine by the following methods.

- ◆ Our network design, the firewall provides access control to and from the snort box over eth0 and the sniffing interface (eth1) does't have an ip address to route to it from the internet.
- ◆ Shutdown of non-essential services and setting up of the appropriate permissions/security for the newly installed software.
- ◆ Review of security advisors from Redhat for our installed packages.
- ◆ Running of the Bastille script.

The following links provide good references to building secure linux servers.

<http://www.openna.com/>

Securing and Optimising Redhat linux servers

<http://www.sans.org>

Securing Linux Step-by-Step Guide (Generic linux hardening document)

<http://www.hp.com/security/products/linux/>

HP Secure OS Software for Linux (OS based on Redhat Linux)

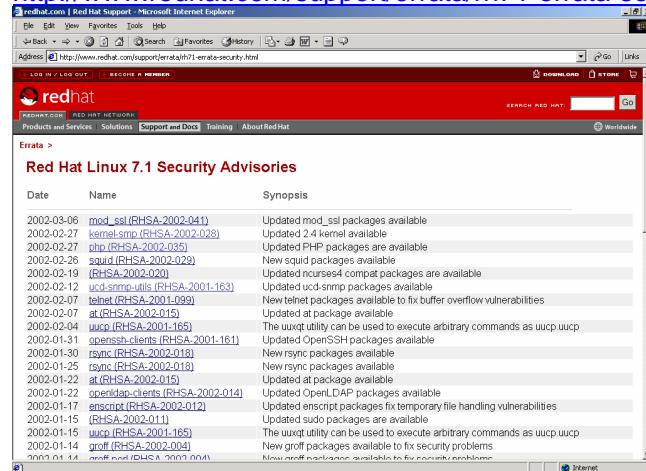
<http://www.linuxfromscratch.org>

Building your own linux distribution from scratch.

### 8.2. Security Patches.

Check the following location for critical security patches that may need to be applied.

<http://www.redhat.com/support/errata/rh71-errata-security.html>



Date	Name	Synopsis
2002-03-06	mod_csi(RHSA-2002-041)	Updated mod_csi packages available
2002-02-27	kernel-2.4.1(RHSA-2002-028)	Updated 2.4 kernel available
2002-02-27	libn (RHSA-2002-035)	Updated FHS packages are available
2002-02-26	squid (RHSA-2002-029)	New squid packages available
2002-03-19	(RHSA-2002-020)	Updated courses4 compil packages are available
2002-02-12	ucd-snmp-libs (RHSA-2001-163)	Updated ucd-snmp packages available
2002-02-07	telnet (RHSA-2001-099)	New telnet packages available to fix buffer overflow vulnerabilities
2002-02-07	at (RHSA-2002-015)	Updated at package available
2002-02-04	uucp (RHSA-2001-165)	The uuxqt utility can be used to execute arbitrary commands as uucp:uucp
2002-01-31	openssh-clients (RHSA-2001-161)	Updated OpenSSH packages available
2002-01-30	rsync (RHSA-2002-018)	New rsync packages available
2002-01-25	rsync (RHSA-2002-018)	New rsync packages available
2002-01-22	at (RHSA-2002-015)	Updated at package available
2002-01-22	openldap-clients (RHSA-2002-014)	Updated OpenLDAP packages available
2002-01-17	encscript (RHSA-2002-012)	Updated encscript packages fix temporary file handling vulnerabilities
2002-01-15	(RHSA-2002-011)	Updated sudo packages are available
2002-01-15	uucp (RHSA-2001-165)	The uuxqt utility can be used to execute arbitrary commands as uucp:uucp
2002-01-14	grort (RHSA-2002-004)	New grort packages available to fix security problems
2002-01-14	www-and-mail (RHSA-2001-099)	New www-and-mail packages available to fix security problems

The following commands are used for package management.

- ◆ rpm -qa (Lists all of the currently installed packages)
- ◆ rpm -qia (Lists all the installed packages with a package description.)
- ◆ rpm -e packagexyz (Removes packagexyz)
- ◆ rpm -i packagexyz (Installs packagexyz)

There are 2 methods to updating the patches.

- ◆ Generate a list of installed packages using the above commands, cross-reference the installed packages with the Redhat security advisories, the advisors provide installation instructions and explanations of the issue. Install the relevant patches
- ◆ Redhat also provide the r2hnetwork service see the following link <https://rhn.redhat.com/help/basic/intro.html>

For a full list of Security Alerts, Bug Fix Alerts, and Enhancement Alerts see the following link.

<http://www.redhat.com/support/errata/rh71-errata.html>

### 8.3. Bastille.

#### Overview.

Bastille is a hardening script for Redhat and Mandrake distributions of linux.

The following packages need to be copied in “/usr/local/acid\_setup\_files” before installing Bastille.

- ◆ Bastille-1.3.0-1.0.i386.rpm
- ◆ Bastille-Curses-module-1.3.0-1.0.i386.rpm
- ◆ perl-Curses-1.05-10.i386.rpm

#### Install.

- ◆ cd /usr/local/acid\_setup\_files
- ◆ rpm -ivh --nodeps perl-Curses-1.05-10.i386.rpm  
(Install the perl Curses library)
- ◆ rpm -ivh --nodeps Bastille-1.3.0-1.0.i386.rpm Bastille-Curses-module-1.3.0-1.0.i386.rpm  
(Install the Bastille scripts)
- ◆ InteractiveBastille  
(Startup command, use the below values)
- ◆ Enter “accept” to accept the conditions
- ◆ Enter yes/no according the below “configure” section
- ◆ Make slight configuration changes (Post-Install Section)
- ◆ Reboot the server for full effect.  
(Don’t reboot until you have made the Post-Install changes)

## Configure.

The following settings are a guide when running Bastille, you can make your own changes depending on your internal security policy.

Bastille Question	Values
Would you like to set more restrictive permissions on the administration utilities?	Yes
Would you like to disable SUID status for mount/umount?	Yes
Would you like to disable SUID status for ping?	Yes
Would you like to disable SUID status for at?	Yes
Would you like to disable SUID status for the r-tools?	Yes
Would you like to disable SUID status for usernetctl?	Yes
Would you like to disable SUID status for traceroute?	Yes
Would you like to prohibit the clear-text r-protocols	Yes

Bastille Question	Values
Would you like to enforce password aging?	Yes
Would you like to restrict the use of cron to administrative accounts?	Yes
Should we disallow root to login on tty's 1-6?	No
Would you like to password-protect the LILO prompt?	No
Would you like to reduce the LILO delay time to zero?	No
Do you ever boot Linux from the hard drive?	Yes
Would you like to write the LILO changes to a boot floppy?	No
Would you like to disable CTRL-ALT-DELETE rebooting?	Yes
Would you like to password protect single-user mode?	No
Would you like to set a default-deny on TCP Wrappers and xinetd?	Yes

Bastille Question	Values
Should Bastille ensure the telnet service does not run on this system?	Yes
Should Bastille ensure the FTP service does not run on this system?	Yes
Would you like to display "Authorized Use" messages at log-in time?	Yes
Please type in the name of the company, person, or other organization who owns or is responsible for this machine.	Entropy Ltd
Would you like to disable the gcc compiler?	Yes
Would you like to put limits on system resource usage?	No
Should we restrict console access to a small group of user accounts?	Yes
Which accounts should be able to login at console?	root
Would you like to add additional logging?	Yes
Do you have a remote logging host?	No

Bastille Question	Values
Would you like to disable apmd?	Yes
Would you like to disable GPM?	Yes
Would you like to deactivate the routing daemons?	Yes
Do you want to stop sendmail from running in daemon mode?	Yes
Would you like to run sendmail via cron to process the queue?	Yes

Bastille Question	Values
Would you like to disable the VRFY and EXPN sendmail commands?	Yes
Would you like to disable printing?	Yes
Would you like to install TMPDIR/TMP scripts?	Yes
Would you like to run the packet filtering script?	No

### Post-Install changes.

When running the Bastille script, if you chose the option to “Enable a default deny on TCP-wrappers” this will block ssh access after a reboot. To change this run through the following.

- ◆ cd /etc
- ◆ vi hosts.allow
- ◆ Navigate to above the following line “# Bastille: default deny”
- ◆ Insert the below text no quotes, above the “# Bastille ....” line.  
“sshd: ALL”
- ◆ Save and exit.

When running the Bastille script, if you chose the option to add an “Unauthorised Notice” then run through the following.

- ◆ cd /etc
- ◆ cp /etc/motd /etc/motd\_bak
- ◆ cp -f /etc/issue /etc/motd
- ◆ vi /etc/rc.local
- ◆ Navigate to the bottom of the file.
- ◆ Insert the below text no quotes at the bottom of the rc.local file  
“cp -f /etc/motd /etc/issue”
- ◆ Save and Exit.
- ◆ Reboot the server

## 9. APPENDIX A

---

### 9.1. Further References.

Along with the URL references throughout this document the following document was used.

Installation instructions for ACID

[http://www.whitehats.ca/main/members/Chris/chris\\_acid/chris\\_acid.html](http://www.whitehats.ca/main/members/Chris/chris_acid/chris_acid.html)

### 9.2. Entropy Ltd.

Entropy is a wholly owned Irish company that was set up in June 1993. The company focus is to provide complete Internet Connectivity and Security Solutions including TCP/IP network design and implementation, email integration and e-mail virus scanning, firewall solutions, encryption and digital signature facilities. <http://www.entropy.ie>

### 9.3. Disclaimer.

Use the information in this document at your own risk. I disavow any potential liability of this document. Use of the concepts, examples, and/or other content of this document are entirely at your own risk.

This guide is written in the hope that it will be useful, but without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose.

All copyrights are owned by their owners, unless specifically noted otherwise. Third party trademarks or brand names are the property of their owners. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Naming of particular products or brands should not be seen as endorsements.

#### **9.4. New Versions and Changelog.**

The current official version can always be found at <http://www.entropy.ie>  
**Changelog.**

Version 1.0 - This is the initial release of this document.

Version 1.1 - Using snort-1.8.6 and minor fixes.

##### **Todo List for ver 1.2**

Build with RedHat Linux 7.2, Apache 2.0.x with authentication, later versions of MySQL, PHP and ACID. Setup of SnortSnarf to process portscan.log file and SnortCenter to manage snort rules.

#### **9.5. Feedback.**

Any and all comments on this document are most welcomed.  
These can be sent to [snort@entropy.ie](mailto:snort@entropy.ie).