Building Snort for Mac OS X 10.7 Lion (Server)

Author : Christoph Murauer
Date : 11.11.2011
Version : 1.1
Created using : Apple´s Wiki 3 Server
E - Mail : christoph_murauer@mac.com
Website : http://www.mac.ph

Contents :

1 : Set a firmware password.

Prerequisites for all following steps :

- A Mac which matches the requirements for Mac OS X 10.7 Lion and a broadband internet connection.
- The latest Mac OS X Lion 10.7.2 version from the Mac App Store.
- Optionally the latest Mac OS X Lion 10.7.2 Server extension from the Mac App Store.
- The latest Xcode 4.2.1 version from the Mac App Store.
- Install (there is no Java and no Flash by default) thees things (without the security risk Flash if possible) and create in your home folder a subfolder called Source.

Security starts at the physical access to your machine (who can use your Mac and boot from which media). A firmware password is also known as EFI password or EFI firmware password. Without this password it is some work to change the default boot device.

Set a EFI password :

1. Switch on your Mac and press the option (alt) key.
2. Choose to boot from the Recovery HD.
3. Choose <Utilities => Firmware Password Utility>.
4. Follow the dialog as shown (also if you like to change a existing EFI password).
5. After a reboot set the default boot media using <Apple menu => Preferences ... => Startup Disc>.

The default boot media can only be changed before booting the system if you hold down the option (alt) key, enter the correct EFI password (at this time the QWERTY keyboard layout is used) and press the return key.

Remove a forgotten EFI password :

1. Switch off your machine and remove the power cord.
2. Change the total amount of RAM in your machine (that means, remove or add some RAM). Don´t try that on a MacBook Air.
3. Switch on your Mac (don´t forget the power cord) and press command (cmd) key + option (alt) key + p + r at the same time and hold it down.
4. Wait till you have heared the chime 3 times and release the keys after the third tone (this deletes the PRAM / NVRAM and the old EFI password).
5. After the password is removed you can restore the old RAM configuration and set a new EFI password.

Attention, a EFI password can´t prevent from a reset, a power off or administrative local / remote access (as shown before, like a sudo nvram or like other tools). So

be careful whom you let play around with your machine.

EFI and the use of the Recovery HD of Mac OS X 10.7 Lion :

1. Switch on your Mac and press the option (alt) key.
2. Enter the EFI password and press the return key.
3. Choose to boot from the Recovery HD.
4. Choose the needed utility (restore the system over internet, repair permissions and ACL´s ...) and follow the instructions as displayed.

2 : Use built-in security.

Let´s activate some built-in security features of the operating system.

<Apple menu => Preferences ... > :

<Security => General>

- Select password required <immediately>.
- Select deactivate automatic login.
- Select demand for a administrator password for preferences panes using a lock symbol.
- I use the lock screen feature instead of the function to log out after x minutes of inactivity. Booth things can be combined.
- Select automatic update the list for save downloads (this is Apple´s malware protection XProtect).
- Deselect deactivate „Reboot in Safari“ if the screen is locked. This is the new guest system which boots with a save system only in a Safari session. There is no Flash available and the guest system requires iCloud and a activated Find My Mac.

<Security => FileFault>

- Leave it deactivated - why ? Because it needs CPU time, disc space, RAM and if someone has your account credentials (username & password) or the master recovery key, then all data is decrypted.
- Use Elettra instead of FileFault to protect your informations (we build it later).

<Security => Firewall>

- Click on <start>.
- Click on <Advanced options ... >.
- Deselect block all incoming connections.
- Deselect allow signed software automatically to accept incomming connections.
- Select Activate Stelth Mode.
- Click on <ok>.

- 2 things as information, first the firewall asks if a application was launched the first time and provide the option to accept incoming network connections (then you can choose to allow or deny it and change it also later under <Advanced options ... > if needed). The second is, that the stealth mode protects against a normal ping but not against LAN / WLAN sniffing and also not against network scans with nmap or Nessus - but it is better then to do nothing.

<Security => Privacy>

- Choose self whether you like to allow applications to use your position (the standard setting is deactivated).
- The new guest system and Find My Mac requires activated location services. If you like to use them then select activate location services.

<Energy Saving => Power Supply>

- Select Wake on demand (also known as wake on lan). If the machine is connected to a power supply, if the Airport card supports it and if you are connectet to a Airport Extreme or TimeCapsule (not all configurations will work) this works also for WLAN.

<iCloud / MobileMe>

- Back to my mac requires the password (there is only 1) of your MobileMe or iCloud account. So be careful what you are doing with it and whom you tell it (don´t forget to configure it also on your Airport Express / Extreme or TimeCapsule). The new iCloud service don´t support shard discs on this devices at the moment.
- The new guest system requires a activated Find My Mac.
- Find My Mac requires activated location services.

<Network => Wi - Fi => Advanced options ... => Wi - Fi (the old name for it was AirPort)>

- Select create computer to computer networks.
- Select change network.
- Select activating and deactivating Wi - Fi.
- Click on <ok> and <apply> to change the settings.
- Check the available options if you use other connection types.

<Bluetooth>

- If possible select invisible.
- If you don´t use / need bluetooth then deactivate it.

<Sharing>

- Run only services which you really need and define users which are allowed to use it if possible.

- Check the options of your running services for example the SSH version and the open ports on all router / firewalls. Check also the configuration files off this applications to hide the used software and it´s version.

<Users & Groups => Password>

- Choose a strong password (containing letters, number, special characters, mix upper and lowercase) which noone knows (also not if the person knows you personally) and don´t write it down.
- Also don´t use the same password as you already use on other (public) services. And change the used passwords from time to time.
- You can use the assistant to get a good password.
- Don´t type in informations to remember the password (password hint).
- Deselect user can change the password using the Apple - ID.

<Users & Groups => Guest Account>

- Deactivate the guest account (this is not the same as the new guest system on the login screen).
- Deselect allow guests to login at this computer.
- Deselect allow a guest to access a shared folder.

<Users & Groups => Login Options>

- Choose what you need / prefer.
- Select show menu for fast user switch and select <symbol>, that needs less space in the menu bar.

<Date & Time => Date & Time>

- Select update date & time automatically and use a trusted NTP server like time.euro.apple.com.

<Software Update => Scheduled Checks>

- Select check for updates and use <daily>.
- Select download updates automatically (the updates are downloaded but not installed, a dialog will appear if something new is there to install).

<TimeMachine>

- Select a media to store your backups. As more backups you have as less data you loose if something bad happened.

<Startup Disc>

- Choose the default boot disc and close the lock.
- This preferences pane can also be used to boot from a FireWire disc using the target disc mode.

<Launchpad => Utilities => Kaychain Access> :

<Keychain Access => Preferences ... => General>

- Select show key ring status in menu bar (a new symbol with a lock appears on the right side of the menubar).
- If you leave your machine select this <lock symbol => lock screen>.

<Launchpad => Safari> :

<Safari => Preferences ... => General>

- Deselect open „secure“ files after download.

Reboot your machine and check whether the settings are set as they should be. Then change all other settings for your needs. The settings for the client and the server version are the same.

3 : Your new friend the terminal.

Many people don´t like or hate the terminal but there is no reason for that. Open <Launchpad => Utilities => Terminal> and use <Terminal => Preferences... > to configure the look and feel to fit your needs. Some details about the terminal.

- The default shell is the bash.
- The terminal is case sensitive. This means that there is a big difference to write man, mAn, Man or whatever.
- One command is one line (even I need two or more lines in the text for one command).
- All entered commands are saved in the file .bash_history in your home folder - after you quit the running terminal session.
- You can view and reuse the entered commands by using the arrow keys up and down.
- There is always a space between the command and its options and arguments.
- Options and / or arguments start with - or --.
- At the end of a command you have to press the return key to get a effect.
- Thats enough for the moments.

The missing Library folder :

One of the new things in Mac OS X 10.7 Lion is, that the Library folder in your home folder is hidden. Open your home folder using <Finder => Go To => Home Folder> to check that. Then go back to your terminal window and enter the following command.

chflags nohidden $HOME/Library

Press the return key and go again back to your home folder in <Finder>. Now the Library folder should be there. Congratulations, your first use of terminal was successful. To get more informations about the terminal use the help menu. To get more informations to a command type in the following in a terminal window.

```
man chflags
```

Use instead of chflags the name of the command for which you need more informations.

4 : The Mac GNU Privacy Guard.

GnuPG is the complete and free implementation of the OpenPGP standard as defined in RFC4880. GnuPG allows to encrypt and sign / decrypt and verify data and communication. I know that there are more tools for GnuPG but at the moment there is no working GPGMail plugin for Lion so GnuPG 1.4.11 is enough for the moment.

Download the source code, check the integrity, extract, build and install :

```
cd $HOME/Source
mkdir gnupg
cd gnupg
curl -L ftp://mirror.switch.ch/mirror/gnupg/gnupg/gnupg-1.4.11.tar.gz -o
gnupg-1.4.11.tar.gz

openssl sha1 gnupg-1.4.11.tar.gz
```

SHA1 checksum : bffb0c60b2e702980f7148ee3a060f29adc82331

```
tar -xzvf gnupg-1.4.11.tar.gz
cd gnupg-1.4.11
./configure
```

For more options use : ./configure --help=short

```
make
make check
sudo make install
```

The command sudo requires always a administrator password like the one from your main account.

gpg was installed in /usr/local/bin.

Import existing keys :

The easiest way is to move the directory .gnupg from the old home folder to the new home folder. Don´t forget to backup .gnupg and don´t loose this directory (because your secret key is also in this directory).

Create a new secret and a new public key (see the man pages to revoke a key) :

gpg --gen-key

And follow the displayed dialog.

Modify the configuration file gpg.conf :

cd $HOME/.gnupg
pico gpg.conf

The following thing must be changed.

Line 151 : keyserver-options auto-key-retrieve

With this option gpg tries to download a key from the key server if possible.

Some useful commands in pico.

- Search : press ctrl + w, enter the search text and press return.
- Cursor position : ctrl + c displays the line number.
- Save : ctrl + o and press return.
- Quit : ctrl + x (if something was modified then pico ask to save or not).

Manage the public (pubring.gpg) and secret (secring.gpg) keys if needed :

gpg --list-secret-keys --fingerprint
gpg --list-public-keys --fingerprint
gpg --delete-key NAME

NAME = are the 8 characters in the first line between the / and the first date. To delete secret keys check man gpg.

Test whether gpg works as it should :

Before we checked the integrity of gpg with a SHA1 checksum. Never ever check gpg with itself. Now after installing we can do that to test gpg.

```
gpg --verify gnupg-1.4.11.tar.gz.sig gnupg-1.4.11.tar.gz
```

This should bring an error which tells you that there is no key on the key server. The reason is that the key which was used for signing is already expired. We download now a .sig file to test it.

```
cd $HOME/Source/gnupg
curl -L ftp://mirror.switch.ch/mirror/gnupg/gnupg/
gnupg-1.4.11.tar.gz.sig -o gnupg-1.4.11.tar.gz.sig
gpg --verify gnupg-1.4.11.tar.gz.sig gnupg-1.4.11.tar.gz
```

If all has worked as it should then there appears a text with the message correct / good signature. From now you can use gpg to check the integrity of downloaded files. For more details see the man pages using man gpg.

5 : Snort.

Snort is a open source IDS (Intruder Detection System) / IPS (Intruder Prevention System) from the company Sourcefire Inc., which can monitor the whole network traffic and report intrusion attempts in single machines or whole networks.

Optionally to update from Snort 2.9.1 to Snort 2.9.1.2 :

If you have no old Snort installed start below this point.
Backup the configuration files from /etc/snort.
Remove the old installation.

```
cd $HOME/Source/snort/snort-2.9.1
```

The following command works only if you don´t run a make clean or make distclean before - otherwise a rerun of configure (with the original options) is necessary. Created directories arn´t removed.

```
sudo make uninstall
cd $HOME/Source/daq/daq-0.6.1
```

The following command works only if you don´t run a make clean or make distclean before - otherwise a rerun of configure (with the original options) is necessary. Created directories arn´t removed.

```
sudo make uninstall
cd $HOME/Source/pcre-8.12
```

The following command works only if you don´t run a make clean or make distclean before - otherwise a rerun of configure (with the original options) is necessary. Created directories arn´t removed.

sudo make uninstall

The old source code tar balls are still there if you haven´t deleted them before.

Download the source code, check the integrity, extract, build and install :

cd $HOME/Source
mkdir libdnet
cd libdnet
curl -O http://libdnet.googlecode.com/files/libdnet-1.12.tgz
openssl sha1 libdnet-1.12.tgz

SHA1 checksum : 71302be302e84fc19b559e811951b5d600d976f8

tar -xzvf libdnet-1.12.tgz
cd libdnet-1.12
./configure && make && make check && sudo make install
cd $HOME/Source
mkdir pcre
cd pcre
curl -O ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-8.20.tar.gz

curl -O ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-8.20.tar.gz.sig

gpg --verify pcre-8.20.tar.gz.sig pcre-8.20.tar.gz
tar -xzvf pcre-8.20.tar.gz
cd pcre-8.20
/configure --enable-jit --enable-utf8 --enable-unicode-properties --enable-pcregrep-libz --enable-pcregrep-libbz2

make && make check && sudo make install
cd $HOME/Source
mkdir daq
cd daq
curl -O -L http://www.snort.org/dl/snort-current/daq-0.6.2.tar.gz
curl -O -L http://www.snort.org/dl/snort-current/daq-0.6.2.tar.gz.sig
gpg --verify daq-0.6.2.tar.gz.sig daq-0.6.2.tar.gz
tar -xzvf daq-0.6.2.tar.gz

```
cd daq-0.6.2
./configure && make && make check && sudo make install
```

For more options use : ./configure --help=short

```
cd $HOME/Source
mkdir snort
cd snort
curl -O -L http://www.snort.org/dl/snort-current/snort-2.9.1.2.tar.gz
curl -O -L http://www.snort.org/dl/snort-current/snort-2.9.1.2.tar.gz.sig
gpg --verify snort-2.9.1.2.tar.gz.sig snort-2.9.1.2.tar.gz
tar -xzvf snort-2.9.1.2.tar.gz
cd snort-2.9.1.2
./configure --enable-sourcefire
```

For more options use : ./configure --help=short
If you like to have a own user and a own group like _snort use the Server Admin Tools for 10.7 to create it (it is possible but not required).

```
make && make check && sudo make install
```

snort was installed in /usr/local/bin.

Test Snort over AirPort as sniffer :

For other devices use ifconfig in terminal.

```
sudo snort -de -i en1
```

Open a website in Safari and look whether data packets are shown in the open terminal window. If all works then you can stop Snort with ctrl + c.

Download the latest rules from snort.org :

A registration and a login on https://www.snort.org/snort-rules is required to download the rules. The subscriber release is a paid service and available in realtime. The registered user release is free of charge but is always released 30 days after the subscriber release. The content of booth versions is the same. Download the files snortrules-snapshot-2912.tar.gz and snortrules-snapshot-2912.tar.gz.md5.txt from the subscriber release or the registered user release section. Move the files from <Downloads> to <Home Folder/Source/snort>.

```
cd $HOME/Source/snort
openssl md5 snortrules-snapshot-2912.tar.gz
more snortrules-snapshot-2912.tar.gz.md5.txt
tar -xzvf snortrules-snapshot-2912.tar.gz
sudo mv ./etc /etc/snort
sudo mv ./preproc_rules /etc/snort/preproc_rules
```

sudo mv ./rules /etc/snort/rules
sudo mv ./so_rules /etc/snort/so_rules
sudo chown -R root:wheel /etc/snort

Modify the configuration file snort.conf :

sudo pico /etc/snort/snort.conf

The following things must be changed.

Line 101 : var RULE_PATH /etc/snort/rules
Line 102 : var SO_RULE_PATH /etc/snort/so_rules
Line 103 : var PREPROC_RULE_PATH /etc/snort/preproc_rules
Line 403 : preprocessor sfportscan: proto { all } memcap { 10000000 } sense_level { low }

Line 406 : preprocessor arpspoof
Line 505 : output alert_syslog: LOG_LOCAL5 LOG_ALERT
Line 593 - 595 : remove the # and the space at the beginning of the line.
Line 603 - 620 : remove the # and the space at the beginning of the line.

Create the directory for the logfiles :

sudo mkdir /var/log/snort

Modify the configuration file syslog.conf :

sudo pico /etc/syslog.conf

To use Syslog we had to add the following line to the configuration file.

local5. /var/log/snort/alert*

Create the directory for the so_rules :

sudo mkdir /usr/local/lib/snort_dynamicrules

Create the files for the reputation preprocessor :

sudo touch /etc/snort/rules/white_list.rules
sudo touch /etc/snort/rules/black_list.rules

Test Snort and the modified snort.conf :

sudo snort -de -i en1 -c /etc/snort/snort.conf

If the message „Commencing packet processing (pid=xxxxx)“ appears then you can stop Snort using ctrl + c.

Using a .plist file and launchd to start Snort at boot time :

To create the file you can use the application you prefer but be sure that you create a plaintext file. So let´s start with the file for Snort.

cd $HOME/Source/snort
pico org.snort.snort.plist

Add the following lines to the file and save it.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Label</key>
        <string>org.snort.snort</string>
        <key>KeepAlive</key>
        <true/>
        <key>RunAtLoad</key>
        <true/>
        <key>ProgramArguments</key>
        <array>
                <string>/usr/local/bin/snort</string>
                <string>-D</string>
                <string>-d</string>
                <string>-e</string>
                <string>-i</string>
                <string>en1</string>
                <string>-c</string>
                <string>/etc/snort/snort.conf</string>
        </array>
        <key>ServiceDescription</key>
        <string>Snort 2.9.1.2 WiFi</string>
</dict>
</plist>
```

Optionally if you need more options use Apples Xcode and the integrated property list editor (if you use binary .plist files still keep the text files for easy editing).

open org.snort.snort.plist

Attention, before we copy the file, we had to change the ownership (for the owner and the group) of it. So if you like to edit the files later use the above commands

with sudo.

```
ls -la
sudo chown root:wheel org.snort.snort.plist
ls -la
```

Copy the file to /Library/LaunchDaemons.

```
sudo cp ./org.snort.snort.plist /Library/LaunchDaemons/
org.snort.snort.plist
```

Reboot your machine. And then we test whether the .plist file was loaded and the application is running or not.

```
sudo launchctl list
ps -u root
```

The -D option for Snort means that it runs as daemon in the background. See also the log files at <Launchpad => Utilities => Console> and there <system.log> or </var/log => snort => alert> for details.

For more informations about Snort see the latest PDF documentation.

6 : Simple WATCHdog.

Simple WATCHdog (also called swatch) is a Perl script which monitors logfiles and sends a e - mails when before defined things happened / are found.

Download the source code, check the integrity, extract, build and install :

```
cd $HOME/Source
mkdir swatch
cd swatch
curl -L http://sourceforge.net/projects/swatch/files/swatch/3.2.3/
swatch-3.2.3.tar.gz/download?use_mirror=switch -o swatch-3.2.3.tar.gz

tar -xzvf swatch-3.2.3.tar.gz
cd swatch-3.2.3
```

Now we use the CPAN shell to install / updated required perl scripts / components. CPAN is the Comprehensive Perl Archive Network.

```
sudo cpan
```

You can let the assistant do the configuration work. To change something on the configuration run one or booth of the following commands (depends whether you like to change the configuration or the used mirrors) at the cpan prompt (cpan[1]>).

o conf init
o conf init urllist

Otherwise we install the required modules.

install Date::Calc
install Date::Format
install Date::Manip
install File::Tail
exit

Now we are back in our standard bash and do the rest of the installation.

perl Makefile.PL
sudo make
sudo make install

swatch was installed in /usr/local/bin.

Create the directory for the configuration files and the configuration file .swatchrc :

sudo mkdir /etc/swatch
sudo pico /etc/swatch/.swatchrc

Enter the following line, modify it to fit your needs and save the file.

```
watchfor /Priority\: 1/i
mail addresses=USERNAME\@DOMAIN,subject=[SNORT] Priority 1 Alert
```

Some explanation of the lines before.

The first line tells swatch to watch for which thing in the log file. Here is it Priority : 1 and the i means to ignore whether it is written in upper or lower case. The second line tells swatch to which e - mail the alert is to sent (modify the USERNAME, the DOMAIN and the text after the = as you need / like).

More options for the configuration file are.

- mail = to send a e - mail.
- exec = to execute a application or script.
- ignore = tells swatch what to ignore in a logfile.

- throttle = tells swatch the interval to do something if the action repeats in a given time. That means for example you find 200 ICMP messages from the same host in 3 minutes in the alert file of Snort. Then you get normally 200 e - mails in 3 minutes. To get only 1 e - mail instead of 200 you can use this option.

For more details see man swatch, the classification file of snort at /etc/snort/classification.config and your alert log file of Snort.

Start swatch as daemon :

sudo swatch --daemon -c /etc/swatch/.swatchrc -t /var/log/snort/alert

The -c option tells swatch where to find the configuration file and the -t option tells swatch which log file to monitor. If swatch send the first e - mail then the application level firewall asks whether the service master should accept incoming connections or not. If you don´t runs your own mail server then you can answer this question with no.

Using a .plist file and launchd to start swatch at boot time :

To create the file you can use the application you prefer but be sure that you create a plaintext file. So let´s start with the file for Snort.

cd $HOME/Source/swatch
pico net.sourceforge.swatch.plist

Add the following lines to the file and save it.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Label</key>
        <string>net.sourceforge.swatch</string>
        <key>KeepAlive</key>
        <false/>
        <key>RunAtLoad</key>
        <true/>
        <key>ProgramArguments</key>
        <array>
                <string>/usr/local/bin/swatch</string>
                <string>--daemon</string>
                <string>-c</string>
                <string>/etc/swatch/.swatchrc</string>
                <string>-t</string>
                <string>/var/log/snort/alert</string>
```

```
        </array>
        <key>ServiceDescription</key>
        <string>Swatch 3.2.3</string>
</dict>
</plist>
```

Optionally if you need more options use Apples Xcode and the integrated property list editor (if you use binary .plist files still keep the text files for easy editing).

open net.sourceforge.swatch.plist

Attention, before we copy the file, we had to change the ownership (for the owner and the group) of it. So if you like to edit the files later use the above commands with sudo.

ls -la
sudo chown root:wheel net.sourceforge.swatch.plist
ls -la

Copy the file to /Library/LaunchDaemons.

sudo cp ./net.sourceforge.swatch.plist /Library/LaunchDaemons/net.sourceforge.swatch.plist

Reboot your machine. And then we test whether the .plist file was loaded and the application is running or not.

sudo launchctl list
ps -u root

You should see a running swatch process and also a running tail process which points to your given log file.