Preparation

With only a few minor exceptions, the majority of this installation guide will take place on the command line using the preinstalled Terminal app.

It is assumed that this is a fresh installation of Mac OS X Yosemite (10.10).

1. If using Safari as the default browser, navigate to its Preferences page and disable (uncheck) the "Open 'safe' files after downloading" box; otherwise, the commands listed below won't work as strictly written if Safari automatically opens them.
2. Navigate to System Preferences > Security & Privacy > and choose to "Allow application downloaded from:" Anywhere, as applications outside the Mac App Store are necessary for installation.
3. For the purposes of this installation guide, the following command will require the root password to be entered and allow the rest of the installation to take place without individual sudo commands being necessary:
4. `sudo bash`

5. Create the following directories:
6. ```
   mkdir /etc/snort
   mkdir /var/log/snort
   mkdir /usr/src
   mkdir -p /usr/local/lib/snort_dynamicrules
   ```

7. Exit and close Terminal completely, and reopen for path changes to take effect.

Installation

Command Line Developer Tools

1. Download and install command line developer tools, necessary to compile packages for OS X.
2. To initiate the download, using Terminal, execute a command that would normally require the command line developer tools, like "gcc".
3. `gcc`

4. You'll receive the following note:
5. `no developer tools were found at '/Applications/Xcode.app', requesting install. Choose an option in the dialog to download the command line developer tools.`

6. You'll then see a dialog box with options to download Xcode or simply install the command line developer tools. Choose the option to Install.
   ```

7. After completing the command line developer tools installation, you will need to close your Terminal session and relaunch, running sudo once more for changes to take effect:
8. `sudo bash`

PCRE

The PCRE (Perl Compatible Regular Expression) library contains the required functionality for linked-applications to implement regular expression matching based on Perl.

The latest version of PCRE can be obtained from http://www.pcre.org/

For the purposes of this installation guide, PCRE 8.36 will be referenced.

DO NOT CONNECT TO FTP SERVER. Download the file below from the mirror site

1. Download pcre-8.36.tar.gz
2. Copy the package into /usr/src
3. `cp ~/Downloads/pcre-8.36.tar.gz /usr/src`

4. Change into the /usr/src directory:
5. `cd /usr/src`

6. Uncompress and unarchive pcre-8.36.tar.gz
7. `tar -zxvf pcre-8.36.tar.gz`

8. Change into the newly created package directory:
9. `cd pcre-8.36`

10. Configure, compile, and install the PCRE library:
11. `./configure`
    `make`
    `make install`

DAQ

The DAQ (Data AcQuisition) library is a data acquisition layer that allows applications to replace direct calls to PCAP and is required by Snort as of 2.9.

The latest version of DAQ can be obtained from http://www.snort.org/downloads

For the purposes of this installation guide, DAQ 2.0.4 will be referenced.

1. Download daq-2.0.5.tar.gz
2. Copy the package into /usr/src
3. `cp ~/Downloads/daq-2.0.5.tar.gz /usr/src`

4. Change into the /usr/src directory:
5. `cd /usr/src`

6. Uncompress and unarchive daq-2.0.4.tar.gz
7. `tar -zxvf daq-2.0.5.tar.gz`

8. Change into the newly created package directory:
9. `cd daq-2.0.5`

10. Configure, compile, and install the DAQ library:
11. `./configure`
    `make`
    `make install`

libdnet

libdnet provides a simplified, portable interface to several low-level networking routines and is required by Snort.

The latest version of libdnet can be obtained from

http://sourceforge.net/projects/libdnet/files/libdnet/libdnet-1.11/

For the purposes of this installation guide, libdnet 1.11 will be referenced.

1. Download libdnet-1.11.tar.gz
2. Copy the package into /usr/src
3. `cp ~/Downloads/libdnet-1.11.tar.gz /usr/src`

4. Change into the /usr/src directory:
5. `cd /usr/src`

6. Uncompress and unarchive libdnet-1.11.tar.gz
7. `tar -zxvf libdnet-1.11.tar.gz`

8. Change into the newly created package directory:
9. `cd libdnet-1.11`

10. Configure, compile, and install the libdnet library:
11. `./configure`
    `make`
    `make install`

Snort

- You can also watch the **Video Tutorial** for this section on YouTube: [13]

Snort is the industry's most widely used and trusted Intrusion Detection and Prevention engine available.

- Note: Interface en0 is being used for this installation guide; substitute the correct interface for your particular system.

The latest version of Snort can be obtained from http://www.snort.org/downloads

The latest rules (those referenced in this guide are 2973) can be obtained from http://www.snort.org/downloads

You must Register on Snort.org to get the rules file.

For the purposes of this installation guide, Snort 2.9.7.3 will be referenced.

1. Download snortrules-snapshot-2970.tar.gz
2. Download snort-2.9.7.3.tar.gz
3. Copy the package into /usr/src
4. `cp ~/Downloads/snort-2.9.7.3.tar.gz /usr/src`

5. Change into the /usr/src directory:
6. `cd /usr/src`

7. Uncompress and unarchive snort-2.9.7.3.tar.gz
8. `tar -zxvf snort-2.9.7.3.tar.gz`

9. Change into the newly created package directory:
10. `cd snort-2.9.7.3`

Compiling

1. Configure, compile, and install Snort with the following commands:
2. `./configure  --enable-gre --enable-mpls --enable-targetbased \`
3. `--enable-ppm --enable-perfprofiling --enable-active-response \`
4. `--enable-normalizer --enable-reload --enable-react`
   `make`
   `make install`

Configuration

1. Copy the default configuration file from the package into the /etc/snort directory:
2. `cp ./etc/* /etc/snort/`

3. nano /etc/snort/snort.conf and make the following changes:

4. `var RULE_PATH /etc/snort/rules`
5. `var SO_RULE_PATH /etc/snort/so_rules`
6. `var PREPROC_RULE_PATH /etc/snort/preproc_rules`
7. `var WHITE_LIST_PATH /etc/snort/rules`
8. `var BLACK_LIST_PATH /etc/snort/rules`
9. Uncomment the Unified2 output line and remove "**nostamp**" from the comma-delimited options list:
10. `output unified2: filename merged.log, limit 128, mpls_event_types, vlan_event_types`
11. Uncompress and install Snort rules:
12. ```
    cp ~/Downloads/snortrules-snapshot-2973.tar.gz /etc/snort/
    cd /etc/snort
    tar -zxvf snortrules-snapshot-2973.tar.gz
    rm -f snortrules-snapshot-2973.tar.gz
    ```
13. Create empty black and white lists:
14. ```
    touch /etc/snort/rules/white_list.rules
    touch /etc/snort/rules/black_list.rules
    ```
15. SID map configuration:
16. ```
    cp /etc/snort/etc/sid-msg.map /etc/snort
    rm -rf /etc/snort/etc
    ```

Starting

Foreground

1. Initially run Snort in the foreground, looking for errors and/or to ensure Snort is properly functioning:
2. `snort -c /etc/snort/snort.conf -i en0`
    ```