Reference Implementation

OpenC2 on OpenSense FW running Hardened BSD 11 on Deciso BV Hardware

Preparation of the image system to develop the build for a complete Hardened BSD 11 and OpnSense with OpenC2 Integration

First create an account on [github.com](http://github.com) and then register and assign OpenC2 as a group to be included.

1. Create a HardenedBSD Image from Full ISO. This can be obtained at the [hardenedbsd.org](http://hardenedbsd.org) site. Obtain the Hardened BSD 11 Current. Download the disc1.iso. Mount and boot from the ISO. Select time zones and select base install.

2. During installation process create a local user to be used to install opnsense. Make a note of the username as it will be needed for sudo.

3. At the local console - login as root after install is complete, several software packages will need to be installed.

4. install pkg by typing # **pkg** and selecting yes at the prompt

5. install git by typing # **pkg install git**

6. install sudo by tying # **pkg install sudo**

7. install libzmq4 by typing # **pkg install libzmq4**

8. install libucl by typing # **pkg install libucl**

9. During the installation, a local user was created. Add the user you created to the sudoers file in **/usr/local/etc/sudoers** and add the following line under the section:

## User privileged specification

**username ALL=(ALL) ALL** , replace username with the username that has been created.

10. generate an ssh key for github access by typing: ssh-keygen -t rsa -b 4096 -C "your\_email@example.com" where the email is the email address used during account creation on github. go to your home folder and go into the .ssh directory and view the id\_rsa.pub file and copy the entire contents. login to github and edit the user profile and go to SSH and GPG key and click New SSH Key. Paste the id\_rsa.pub key there

Preparing the image build process and getting OpenC2 functionality integrated

Log into the Hardened BSD OS and sudo to root

Obtain the HardenedBSD source for building OpenC2 Opnsense. This process takes upwards of 30 minutes to download.

If you are at the console, everything can be done as root - however if the procedures are run remotely via SSH then login as the user account created and execute everything with a sudo command in front of each command, especially if there is is no way to sudo to root either.

Step 1. Once logged into the system go to the following directory

# **cd /usr/src**

Step 2.Run the following command to get the HardenedBSD source

:/usr/src # **git clone git://github.com/HardenedBSD/hardenedBSD-playground.git .**

*Output will be the following (and takes upwards to 30 minutes or more)*

*Cloning into '.'...*

*remote: Counting objects: 2341180, done.*

*remote: Compressing objects: 100% (3911/3911), done.*

Step 3. Run the following checkout process

/usr/src # **git checkout -b hardened/experimental/opnsense-master origin/hardened/experimental/opnsense-master**

Output will be the following:

*Branch hardened/experimental/opnsense-master set up to track remote branch hardened/experimental/opnsense-master from origin.*

*Switched to a new branch 'hardened/experimental/opnsense-master'*

Installation of OpenSense. Follow the steps exactly

Obtain Opnsense Tools:

# **mkdir /usr/tools**

# **cd /usr/tools**

# **git clone [git@github.com](mailto:git@github.com):OpenC2-org/opnsense-tools .**

Obtain Opnsense Ports:

# **mkdir /usr/ports**

# **cd /usr/ports**

# **git clone [git@github.com](mailto:git@github.com):OpenC2-org/opnsense-ports .**

Obtain Opnsense Core:

# **mkdir /usr/core**

# **cd /usr/core**

# **git clone [git@github.com](mailto:git@github.com):OpenC2-org/opnsense-core .**

Return to the user home directory to obtain the openc2 files: For the documentation - the home directory is /home/openc2

# **mkdir /home/openc2/openc2-orchestrator**

# **cd /home/openc2/openc2-orchestrator**

# **git clone git@github.com:OpenC2-org/openc2-orchestrator.git .**

# **mkdir /home/openc2/openc2-broadcast**

# **cd /home/openc2/openc2-broadcast**

# **git clone git@github.com:OpenC2-org/openc2-broadcast.git .**

# **mkdir /home/openc2/openc2-edge**

# **cd /home/openc2/openc2-edge**

# **git clone [git@github.com](mailto:git@github.com):OpenC2-org/openc2-edge.git .**

# **mkdir /home/openc2/openc2-edge-allow**

# **cd /home/openc2/openc2-edge-allow**

# **git clone git@github.com:OpenC2-org/openc2-edge-allow.git .**

# **mkdir /home/openc2/openc2-edge-deny**

# **cd /home/openc2/openc2-edge-deny**

# **git clone git@github.com:OpenC2-org/openc2-edge-deny.git .**

Create an Openc2 Orchestrator distribution file

obtain the distribution file

cd /usr/ports/g2/openc2-orchestrator

view the distinfo file in the directory to see how the file should be retrieved

/usr/ports/g2/openc2-orchestrator # **more distinfo**

SHA256 (openc2-orchestrator-0.0.0.2016030701.tar.gz) = 152074d988461b1329bf0b89a0c04255774e3e36281e5c9d9f8c827f1d09932f

SIZE (openc2-orchestrator-0.0.0.2016030701.tar.gz) = 2082

the name is the following

openc2-orchestrator-0.0.0.2016030701.tar.gz

Create a directory where the file will be created:

# **mkdir /usr/local/distfiles**

Create the openc2-orchestrator file by running the following commands:

# **cd /home/openc2/openc2-orchestrator**

# **git archive --format=tar.gz -o /usr/local/distfiles/openc2-orchestrator-0.0.0.2016030701.tar.gz --prefix=openc2-orchestrator-0.0.0.2016030701/ HEAD**

Installation of OpenC2 functions

Run the following in order to integrate the OpenC2 functionality into OpnSense

# **cd /home/openc2/openc2-orchestrator**

# **make depend**

# **make all**

# **make install**

installing broadcast (for opnsense)

# **cd /home/openc2/openc2-broadcast**

# **make depend**

# **make all**

# **make install**

installing edge

# **cd /home/openc2/openc2-edge**

# **make depend**

# **make all**

# **make install**

installing edge-allow

# **cd /home/openc2/openc2-edge-allow**

# **make depend**

# **make all**

# **make install**

installing edge-deny

# **cd /home/openc2/openc2-edge-deny**

# **make depend**

# **make all**

# **make install**

Final steps for configuration

# **mkdir /opnsense**

# **cd /opnsense**

# **mkdir data-work**

# **cd data-work**

# **git clone git@github.com:OpenC2-org/opnsense-data.git .**

**Building the images for installation onto hardware (.img file) to be installed on the OpnSense FW Hardware.**

# **cd /usr/tools/build**

# **/bin/sh ./clean.sh -c /opnsense/data-work/generic.conf packages base kernel images obj stage release**

(this should take less than 30 seconds)

# **/bin.sh .base.sh -c /opnsense/data-work/generic.conf**

(this can take up to 30 hours or longer depending on resources available)

# **/bin/sh ./kernel.sh -c /opnsense/data-work/generic.conf**

(this can take several hours to complete)

# **/bin/sh ./ports.sh -c /opnsense/data-work/generic.conf**

(this can also take several hours to complete)

# **/bin/sh ./core.sh -c /opnsense/data-work/generic.conf**

# **/bin.sh /memstick.sh -c /opnsense/data-work/generic.conf**

Navigate to the follow directory to find two builds ready for installation at the following location

# **cd /opnsense/openc2/builds/openc2-exp-01**

Two files should be here

HardenedBSD-openc2-exp-01\_OPNSense-serial-amd64.img

HardenedBSD-openc2-exp-01\_OPNSense-vga-amd64.img

On the linux or Mac using the dd command to make an copy of the serial or VGA image onto a USB. Once the image has been loaded into the USB, insert it into one of the USB ports of the firewall and reboot.

It will then go through a normal installation of OpnSense Firewall Installation process.