William J. Heaton
Cryptocybernetics, LLC.
4917 Evergreen Way, #10
Everett, WA 98203
wjh@conflux.net
(425) 710-9006

How to Harden Snow Leopard

"Installing a full featured internet server on Mac Mini using OS/X 10.6"

May 7, 2010

Table of Contents

Introduction

When the first Mac Mini was produced by Apple in January, 2005 we immediately thought that it would make a marvelous server for our ISP. Over the years the Mac Mini has become a stable foundation for our servers. Our first servers were based on the Mac OS/X Server but having an Operating System that cost more than the hardware was a bit unsettling.

In February, 2005 Nerd Vittles wrote a five part series: "ISP-In-A-Box: The $500 Mac mini" and that was the genesis of this document..

Most of the hardening techniques used in this document are derived from "Mac OS X -- Security Configuration For Version 10.5 Leopard Second Edition" currently found at: http://www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml along with best practices that I've discovered from using Mac Minis as servers since they came out.

Caveat

This document is oriented towards an experienced OS/X system administrator and is not for the faint of heart. It is tailored for a specific working environment that requires a fair bit of esoteric knowledge to maintain.

If you do not have this experience, I highly recommend that you consider using the Apple OS/X Server which is sufficient for most installations. The list price is currently $499 from Apple and you can find copies on eBay for 2-3 hundred dollars.

Installation

This Installation guide uses the stock Mac mini "Mac OS X Install DVD" for "Mac OS Version 10.6 version 1.0" Occasionally Apple will refresh the installation media so don't be surprised if your details may very slightly. The object of this section is to get the minimal initial system installation in place and the have the latest System Updates applied.

IPL (Initial Program Load)

The default OS/X install takes over the entire disk. While OS/X is extremely robust, the occasional failure tends to cause problems on the boot volume. We change the default scheme to allow for a second boot partition and a separate partition to store user files.

- Boot using the OS/X Install DVD.
- At the first screen use the "Utility" menu to start the "Disk Utility." Split the disk into three partitions: "Boot1" with 40gb of space, "Boot2" with 40gb of space, and "Home" using the rest of the disk.

Note: The size of the boot partitions I use is a compromise. The smaller the boot partitions the more often you'll need to trim back logs and temporary files. The larger the partition the more you take away from the user files. Values in the range 30gb to 50gb tend to work well.

- Continue with the normal install.
- At the "Install Mac OS/X" screen, select the "Boot1" volume for the installation. Click the "Customize" button and deselect all options. Continue the installation by clicking the "Install" button.

System Setup Screen

Continue through the setup screens. For the most part you don't need to take any action. Don't transfer my information, and don't enter an Apple ID. You don't even need to fill out the "Registration Information" just hit "Continue" or Command-Q to bypass registration.

Create Your Account Screen

The "Create your Account" is the first place that we'll take some proactive steps to improve security. The user you create here will the administrator user for your server. The username should make sense to you however you want to avoid an obvious user name.

Research has shown that the ten most vulnerable usernames are: "root," "admin," "test," "guest," "info," "adm," "mysql," "user," "administrator," and "oracle." All should be avoided.

This account has the keys to the kingdom. A very strong password is appropriate. To give you an idea I use a 14 character password that uses both upper and lower case characters, numbers, and symbols.

Hint: When using the "System"/"Accounts" preference panel to change a user password, notice that the "New Password" field has a key icon at the end of the line. Clicking this icon will invoke the password assistant to help you create a strong password.

I do not recommend setting a password hint. You however may want to put a short notice of how to contact the administrator by email or phone.

Install Software Updates

The very first thing you should do is perform a "Software Update." If the network was auto configured, the system will try to automatically launch the process.

If not, configure the network and then start the update using the "Apple Menu" in the upper left hand corner of the finder window and select "Software Update."

Hint: If the updates contain firmware changes, you may have to reboot to complete the update. If that happens allways make sure to invoke the Software updates until the system tells you that there are no more.

Finder and Desktop Configuration

The Finder and Desktop Configuration are user-centric and we can simplify our world by making them server-centric. This section is optional but recommended.

Finder Preferences

Bring up a Finder window and select “Preferences” from the “Finder” menu. Set the options for each of the tabs as follows

General

- "Show these items on desktop"
  - ☑ Hard disks.
  - ☑ External disk.
  - ☑ CDs, DVDs, and iPods.
  - ☑ Connected Servers
- "New Finder windows open"
  - ☐ "xxx's Mac Mini" (i.e. The Computer which is usually the first item)

Labels

No Changes.

Sidebar

- ☑ Devices — **Select** all checkboxes except iDisk.
- ☑ Shared — **Deselect** all checkboxes.
- ☑ Places — **Select** all Checkboxes.
- ☑ Search for — **Deselect** all Checkboxes.

Advanced

Select all Checkboxes.

- ☑ Show all filename extensions
- ☑ Show warning before changing an extension
- ☑ Show warning before emptying the Trash
- ☑ Empty Trash Securely.

Desktop

You should now have the disk volumes on your desktop. We'll set the label colors to give a visual cue of the system vs user files.

- ☐ Control-Click on "Boot1" and "Boot2" and set label color to "Red."
- ☐ Control-Click on "Home" and set label color to "Green."
- ☐ Control-Click on Desktop and "Show View Options" and set to taste.

Toolbar

We're removing the user-centric applications from the toolbar and replace them with a set that are of more use to a system administrator. All applications are located in "Applications" and "Applications/Utilities" directories on the boot volume.

Applications to remove

- ☐ Mail.
- ☐ iChat.
- ☐ Address Book.
- ☐ iCal.
- ☐ iTunes.
- ☐ PhotoBooth.

Applications to add

- ☐ TextEdit.
- ☐ Utilities/Activity Monitor.
- ☐ Utilities/Console.
- ☐ Utilities/Disk Utility.
- ☐ Utilities/System Profiler.
- ☐ Utilities/Terminal.
- ☐ System Preferences.

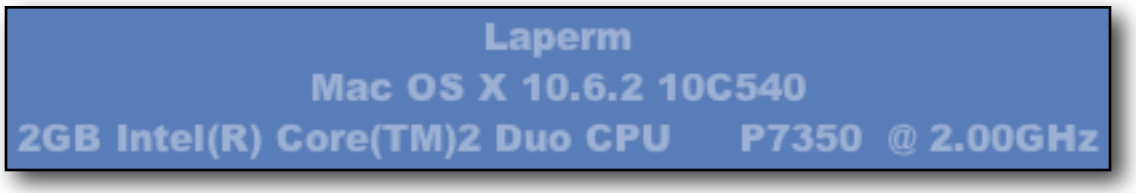
GeekTool

GeekTool is a System Preferences module for Mac OS that lets you display on your desktop three different types of information: files, images, and the results of shell commands. You can find geektool at http://projects.tynsoe.org/en/geektool/

I use the following shell geeklet:

```
sscutil --get ComputerName;
sw_vers | awk -F':\t' '{printf $2 " "}' | paste -d ' ' - - -;
sysctl -n hw.memsize | awk '{printf $0/1073741824"GB "}';
sysctl -n machdep.cpu.brand_string;
```

To display the basic system information just above the toolbar:



Setting System Preferences

Personal

Appearance

No Changes.

Desktop & Screen Saver

The object here is to make the screen as simple as possible so that using Remote Desktop or IP Consoles are as fast as possible. We're effectively disabling the screen saver to reduce a bit of load on the server.

Desktop

- ☐ **Select** one of the solid colors.
- ☑ **Deselect** "Translucent Menu Bar"

Screen Saver

- ☑ **Deselect** "Use random screen saver," "Show with clock"
- ☑ **Select** "Apple/Computer Name" screen saver
- ☐ **Set** "Start Screen saver" to "Never"

Dock

We're turning these off to speed up Remove Desktop.

- ☑ **Deselect** "Magnification"
- ☑ **Deselect** "Animate opening applications"

Exposé & Spaces

We're turning these off to reduce confusion when accessing remotely.

Expose

- ☐ **Set** all fields to "-"

Spaces

- ☑ **Deselect** "Enable Spaces"
- ☑ **Deselect** "Show Spaces in menu bar"
- ☐ **Set** all other fields to "-"

Language & Text

No Changes.

Security

We're maximizing the security options. Note: The firewall options will be most likely be modified later, for now we're just defaulting to no access.

General

- ☑ **Select** "Require Password"
- ☑ **Select** "Disable automatic login"
- ☑ **Select** "Logout after" 60 minutes of inactivity
- ☑ **Select** "Disable remote control infrared receiver"

FileVault

No Changes.

Firewall

- **Click** "Start"
- **Click** "Advanced"
  - ☑ **Select** "Block All incoming connections" Note: May get changed in a later chapter.
  - ☑ **Deselect** "Automatically allow signed software to receive incoming connections"

Spotlight

We're turning off spotlight to reduce processor load.

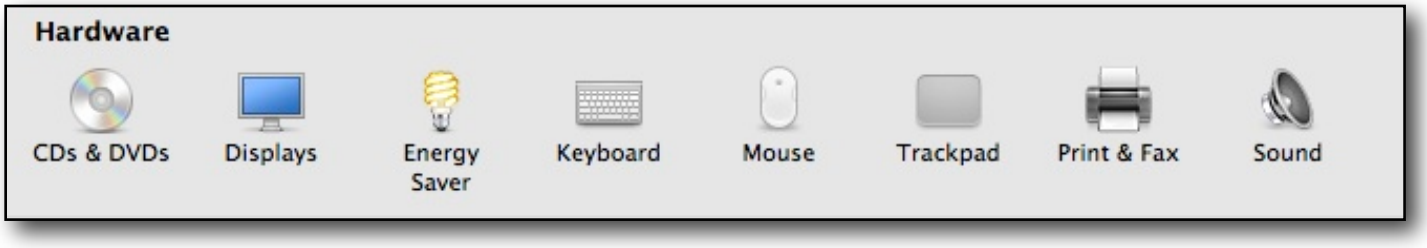
Search Results

- ☑ **Deselect** all fields.

Privacy

- ☐ **Add** Volumes "Boot1," "Boot2," and "Home" (Yes you are sure)

Hardware



CDs & DVDs

We don't want any automatic options with the removable media.

- ☐ **Set** all fields to "Ignore"

Displays

We do want to have control of the display in the toolbar.

- ☑ **Select** "Show Display in menu bar"

Energy Saver

Configure the Power settings to ones more appropriate for a server.

- ☐ **Set** Computer Sleep to "Never"
- ☐ **Set** Display Sleep to "15 Minutes"
- ☑ **Deselect** "Allow power button to put the computer to sleep"
- ☑ **Select** "Startup automatically after a power failure"

Keyboard

No surprise shortcuts because we'll probably we accessing the server remotely.

Keyboard

No Changes.

Keyboard Shortcuts

- ☑ maximizing all shortcuts.

Mouse

No Changes.

Print & Fax

No Changes.

Sound

Computer Rooms tend to be noisy!

Sound Effects

- ☐ **Set** Alert Volume to Maximum

Output

No Changes.

Input

- ☐ **Set** Input Volume to Minimum

Internet & Wireless

MobileMe

MobileMe doesn't make sense for a server. The default is disabled.

No Changes.

Network

We only allow access through the ethernet port.

Ethernet

- ☐ Configure as needed

Firewire

- ☐ Under advanced: **Set** "Configure IPxx" to "Off"

Airport

- ☐ **Click** "Turn Airport Off"
- ☑ **Deselect** "Show Airport Status in Menu Bar"
- ☑ Advanced: **Select** all options.

Bluetooth

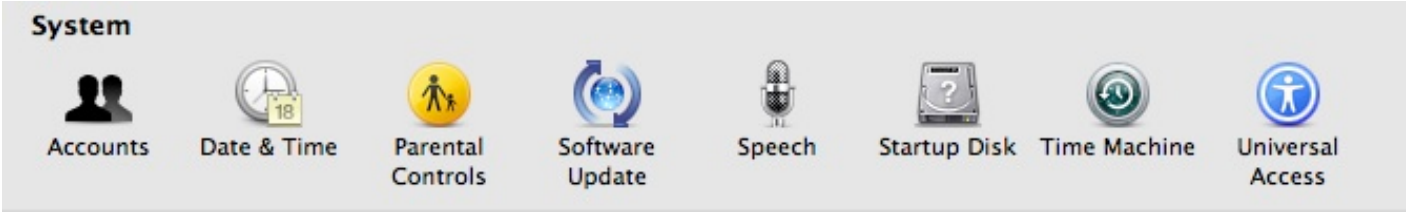
We don't allow access through Bluetooth.

- ☑ **Deselect** "On"
- ☑ **Deselect** "Discoverable"
- ☑ **Deselect** "Show Bluetooth status in the menu bar"
- ☑ Advanced: **Deselect** all items.

Sharing

- ☐ **Set** Computer Name (and in "Edit…")
- ☑ Deselect All Services. *Note: Some may be enabled in later chapters.*

System



Accounts

Login Options

- [ ] **Set** Automatic Login: "Off"
- [ ] **Set** Display Login Window as: "Name and Password"
- [x] **Deselect** all checkboxes

Admin Account

No Changes.

Guest Account

- [x] **Deselect** "Allow Guests to connect to shared folders"

Parental Controls

No Changes.

Software Update

- [ ] Set “Check for updates:” to "Daily"

Speech

No Changes.

Startup Disk

No Changes.

Time Machine

No Changes.

Universal Access

No Changes.

Access Messages

Access messages are used to discourage unauthorized server access, remind users of security awareness, and for providing a legal basis for prosecution in cases involving unauthorized access. I recommend that your research what is appropriate for your situation.

We use the following message:

```
Unauthorized access is prohibited and will be prosecuted.
All accesses are monitored and/or recorded.
```

Login Screen

- ☐ From a Terminal Session:

```
sudo defaults write /Library/Preferences/com.apple.loginwindow \
LoginwindowText "Access Warning"
```

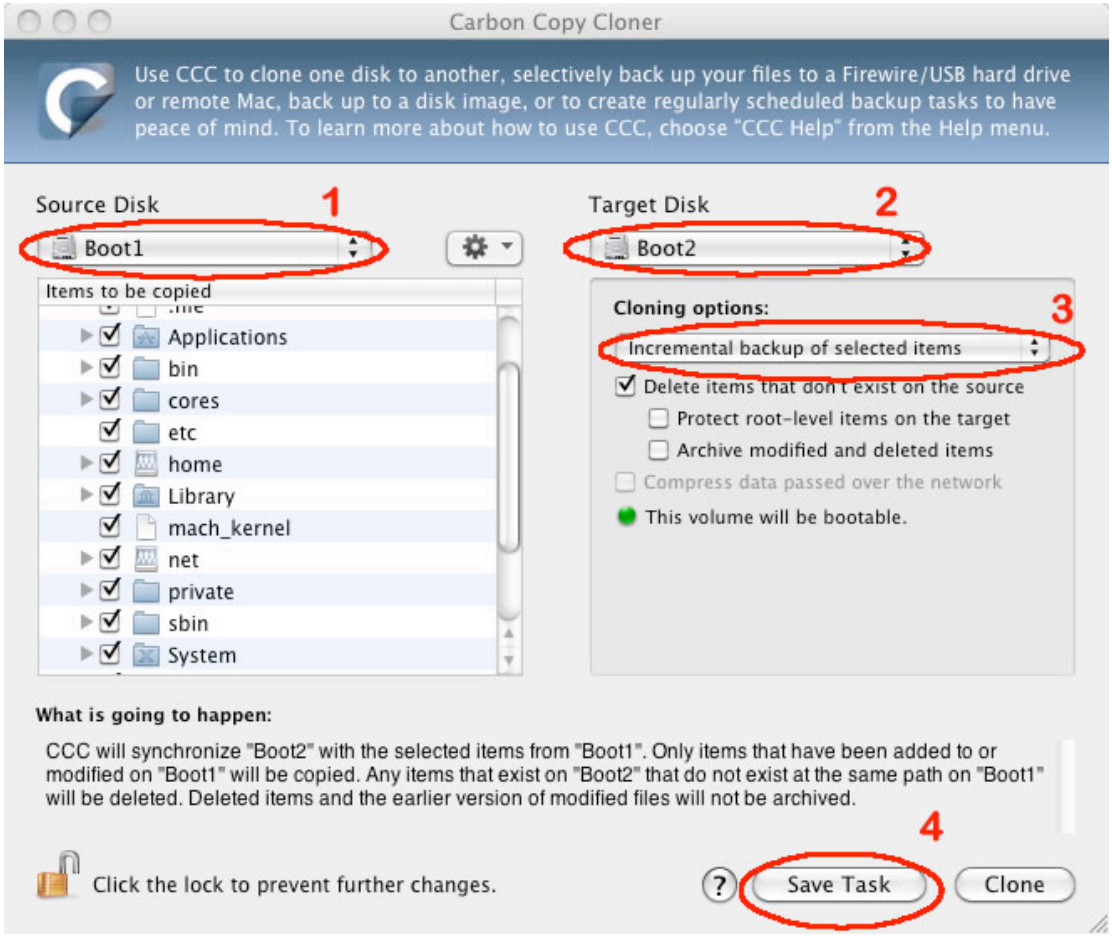
Shell Access

- ☐ From a Terminal Session:

```
sudo vi /etc/motd
[Add Access Warning]
```

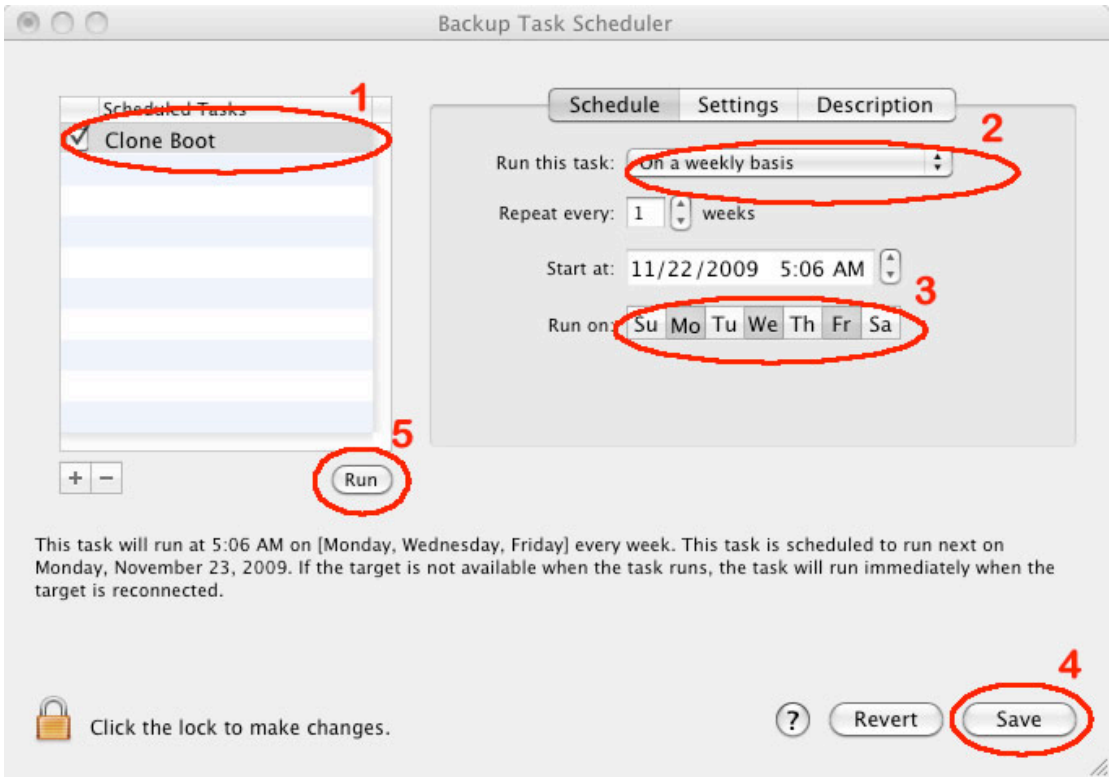
Carbon Copy Cloner

Carbon Copy Cloner (CCC) from http://www.bombich.com has been one of the must-have utilities for Mac users since the early days of OS X. We use CCC every other day to create a bootable copy of the Boot1 volume.



Setting up the clone

1) **Set** "Source Disk" to "Boot1"
2) **Set** "Target Disk" to "Boot2"
3) **Select** "Incremental backup of selected items"
4) **Click** "Save Task"



Scheduling the operation

1) Rename the task to "Clone Boot" by **double clicking**.
2) **Set** "Run this task" to "Select on a weekly basis"
3) **Select** "Mo", "We", and "Fr"
4) **Click** "Save"
5) **Click** "Run" to create the initial run

Basic Web Server (Optional)

Most servers eventually end up needing a basic Web Server so even if you don't need one right now, you may want to bring it up to a reasonable level and then disable it.

We're doing three things. Turning on PHP, Relocating the web files over to the Home volume, and disabling the user webs (i.e. xxxx.com/~admin.)

Finally we create a simple default website that serves as an "Access Denied" page.

Configure Apache

- **Copy** /etc/apache2/httpd.conf to /etc/apache2/httpd.conf.dist
- **Edit** /etc/apache2/httpd.conf' (Must be root)

☐ (Optional) Enable PHP: Remove comment at approximately line 115.

```
LoadModule php5_module        libexec/apache2/libphp5.so
```

☐ Change DocumentRoot at approximately line 167.

```
DocumentRoot "/Volumes/Home/Web/Default"
```

☐ Replace <Directory "/Library/WebServer/Documents"> block at approximately line 194.

```
<Directory "/Volumes/Home/Web/Default">
    Options FollowSymLinks MultiViews
    AllowOverride All
    Order allow,deny
    Allow from all
</Directory>
```

☐ Disable User Directories: Comment out at approximately line 436.

```
#Include /private/etc/apache2/extra/httpd-userdir.conf
```

Create Default website

- [ ] **Create** the directory "/Volumes/Home/Web/Default"
- [ ] **Create** index.php (Note: Requires PHP to be enabled)

```
<html>
  <head>
    <meta http-equiv="Content-Language" content="en-us">
    <meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
    <title>Access Denied</title>
     <style>
       div#note  { margin: 0 auto; width:600px; background-color:#005c8a;
                   color:white; text-align:center;}
       div#name  { font: 1.5em "Arial Bold"; }
       div#legal { font: 1.0em "Arial Alternative"; }
     </style>
  </head>

  <body>
    <div id="note">
      <div id="name"><?= php_uname("n");?></div>
      <div id="closed">
        <img border="0" src="closed.jpg" alt="" width="600" height="402" />
      </div>
      <div id="legal">
        Access to this site is restricted to authorized personnel only.
      </div>
    </div>
  </body>
</html>
```

- [ ] **Copy** "closed.jpg" into the directory.

Activate Web Sharing

System Preferences/Security

Advanced

☑ **Deselect** "Block all incoming connections"

System Preferences/Sharing

==========

☑ **Select** "Web Sharing"

Note: The "Personal Website" link should not work. The "Computer" website should work. Be sure to test both remotely and locally.

SSH Hardening

SSH is one of the largest targets of opportunity for hackers. The object here is to reduce the SSH default footprint to the minimum possible.

> *Note: We use port 2222 for this example. You may want to pick another port. Be sure to research that it doesn't conflict with other important services that you may want to use.*

Update SSH Configuration

- **Copy** /etc/sshd_conf to /etc/sshd_confiig.dist
- **Edit** /etc/sshd_config (Must be root)
  - Uncomment and change port number.

```
Port 2222
```

  - Uncomment and turn off root login.

```
PermitRootLogin no
```

  - Uncomment and change MaxAuthTries.

```
MaxAuthTries 2
```

Move SSH port

- **Copy** /System/Library/LaunchDaemons/ssh.plist to /System/Library/LaunchDaemons/ssh.plist.dist
- **Edit** /System/Library/LaunchDaemons/ssh.plist (Must be root)
  - Locate line following "SockServiceName" and change service name:

```
<string>ssh2</string>
```

Define the SSH2 service

- **Copy** /etc/services to /etc/services.dist
- **Edit** /etc/services (Must be root)
  - Locate lines for ssh and add the ssh2 service:

```
ssh2        2222/udp    # Private SSH port
ssh2        2222/tcp    # Private SSH port
```

Update SSH Sandbox

- **Copy** /usr/share/sandbox/sshd.sb to /usr/share/sandbox/sshd.sb.dist
- **Edit** /usr/share/sandbox/sshd.sb (Must be root)
  - **Add** to the end of the file:

```
(allow mach-per-user-lookup)
```

Enable SSH

System Preferences/Security

Advanced

- [x] **Deselect** "Block all incoming connections"

System Preferences/Sharing

- [x] **Select** "Remote Login"
- [x] **Select** "Only these Users"
- [ ] **Add** the Admin user.