Old Dominion University's Information Technology Services MAC OS X Workstation Hardening Guide

The purpose of this guide is to assist self-administrated MAC OS X Workstation users secure their systems.

This guide makes the following assumptions:

- You know how to install and configure MAC OS X
- You follow the MAC OS X best practices as set down by Apple
- You are using a anti-virus protection suite for MAC. You can get McAfee from ITS here:
    - http://www.odu.edu/ts/software-services/mcafee-win

Steps to follow to harden your system:

1) Disable Bonjour's multicast advertisements with the following command and reboot:
    a. sudo defaults write /System/Library/ LaunchDaemons/com.apple.mDNSResponder ProgramArguments -array-add "-NoMulticastAdvertisements"
2) Disable Automatic Login and User List:
    a. Click on "Login Options." Set "Automatic login" to "Off." Set "Display login window as" to "Name and password."
3) Disable guest account and sharing:
    a. Select the Guest Account and then disable it by unchecking "Allow Guest to log in to this computer." Uncheck "Allow guests to connect to shared folders."
4) Open the Security pane in System Preferences. In the General tab, ensure that the following are checked:
    a. Require password "5 seconds" after sleep or screen saver begins
    b. Disable automatic login
    c. Use secure virtual memory
    d. Disable Location Services (if present)
    e. Disable remote control infrared receiver (if present)
5) Turning On File Extensions
    a. Open Finder.
    b. From the Finder menu, select Preferences.
    c. Click Advanced and select the "Show all filename extensions" checkbox.

6) Set Global Password Policies
    a. This will set the global password policy to be: minimum of 12 characters and have no more than 3 failed attempts:
        i.
        ```
        $ pwpolicy -n /Local/Default -setglobalpolicy "minChars=12 maxFailedLoginAttempts=3”
        ```

ITS best practice recommendations

1) Do not log onto your computer with an administrator account for normal day to day use. Use a standard User level account and only use an administrator account for elevation purposes for running or installing trusted software.
2) Install the LANDesk Client software from ITS to keep the software on your machine up to date with the rest of the campus. If you want to take advantage of this service please run the LANDesk installer included with this file.

Reference

1) For more information on further securing your OS X 10.6 system please see:
    a. http://images.apple.com/support/security/guides/docs/SnowLeopard_Security_Config_v10.6.pdf