1. Initial Document

Created By: Michael Carroll (mcarro18@kennesaw.edu)

Document Creation Date: August 21, 2009

2. Revision

Revised By: 2014 OS X Server Security Best Practices Committee

Revision Date: February 17, 2014

Version Number: 0.4

3. Acknowledgements

The Common Security Best Practices portion of this document is based on the Windows Security Best Practices by Brent Williams (bwillia@kennesaw.edu).

The final release document is a collaborative work between the following committee members:

Alicia Flowers Andre Forbes Ray Kerce

4. Usage

This document is intended to serve as a general guideline and should not be interpreted as policy. Furthermore, the ever changing nature of information technology prevents this document from being entirely inclusive but should serve as a general baseline for server installation. Please feel free to query the System Administrators Group and ListServe for additional guidance.

Table of Contents

5. Common Security Best Practices

5.1 Physical Security and Reliability

5.1.1 Limited Access

Servers should always be located in a secured, locked area that ideally is equipped with cardkey access. Should an intruder gain access to a server console, it is possible that serious damage or data theft could occur. This could be done directly through the server console or by potentially booting the server with a "Live CD" that allows easy access to server hard drives.

5.1.2 Redundant Power

All servers should be operated from redundant power systems (UPS.) This is for protection of the server hardware (offering some isolation from power surges, sags and spikes), and to protect information on server hard drives by allowing the server to be gracefully powered down in an extended power outage. How long the redundant power system can power servers in a power failure is a function of the criticality of the servers. In non-critical, academic settings, a few minutes of redundant power may be all that is needed to smooth over a brief outage. However, for mission critical servers, it may be necessary to provide the capability of 24 by 7 redundant power.

5.1.3 Fire Control

Servers should not be placed in an area covered by a fire suppression sprinkler system. In such circumstances, even a minor fire can result in complete loss of servers and storage devices. Instead, server rooms should employ a Halon or similar fire suppression system.

5.1.4 Climate Control

Server hardware is most reliable when it is operated in a cool environment. If your server room is too warm, seek assistance from campus physical plant operations to determine how the room can be better cooled.

5.1.5 Redundant Servers

Whenever possible, failover servers should be in place to prevent downtime in the case of a disaster.

5.1.6 Clustering and Failover

If the operation of your servers is critical, you may want to consider server clustering and/ or server failover. Most server software is capable of both. Ideally, server hardware should be as identical as possible.

5.1.7 Redundant Storage

Server hard drives are heavily used, it's important that some form of redundant storage be provided. It is not unusual to have a single hard drive failure in a file server. Various methods for protecting against such failures are available and should be employed.

5.1.8 RAID

Most servers support redundant storage in two ways. Two or more drives can actually be installed in a server and drive mirroring or a stripe set with parity can be configured. Optionally, redundant storage hardware can be purchased from many vendors. These redundant storage systems appear to a server as a single drive but do provide continued operation in the event of a single drive failure.

5.2 Disaster Recovery Practices

5.2.1 Backups

It is very important that servers are backed up on a regular basis. In most environments it is adequate to perform backups on a weekly basis but criticality may dictate a different schedule.

5.2.2 Off-site Backup Storage

It's very important that one backup set be taken off site on a regular basis. This is to prevent a total loss should the physical facility be lost in a fire or other natural disaster.

5.2.3 Testing a Backup

It is critical that a backup set occasionally be fully restored to a test system. This is to assure that the backups are occurring as they should and that in fact they can be restored when necessary. It is suggested that a backup set restore be tested once per quarter, but once a month might be appropriate in more critical environments.

5.3 Update Practices

5.3.1 Updates

It is very important that updates and patches be applied to servers in a timely manner after extensive testing for backwards compatibility with production software and systems.

5.4 Security Related Software

Servers are vulnerable to many forms of attack. It's important that a server be equipped with safeguards to protect the information resident on the system and the system itself.

5.4.1 Antivirus and Antispyware

Servers are vulnerable to a variety of malicious software through a number of attack vectors. Having the appropriate antivirus and antispyware tools running on a server and ensuring they remain up to date is extremely important to help combat this problem.

It is strongly encouraged that you use the Microsoft Endpoint Protection Client (MEP) if it's available for your operating system. Please contact iso@kennesaw.edu for more information on the MEP client.

5.4.2 Firewall

Kennesaw State University employs a campus firewall that protects the campus environment from Internet threats. But the campus firewall does nothing to protect servers from threats originating on campus. For that reason, it is reasonable to employ some form of a software firewall on a server.

It is strongly encouraged that you use the built-in firewall, accessible in System Preferences → Security & Privacy. Please contact iso@kennesaw.edu for more information.

5.5 Auditing Practices

5.5.1 Log Retention

Servers keep several logs and, by default, are set to reuse log file entries that are older than seven days. It's a good practice to expand the size of the allowed log file and to set it to reuse space as needed. This allows logging to continue uninterrupted. How far back your log entries go will depend on the size of the log file and how quickly you are accumulating log data. It is strongly encouraged that you keep at least 30 days of logs.

5.5.2 Auditing Practices

Most servers have a powerful auditing feature built in. It is usually disabled by default but can be easily enabled. Typically, server managers would want the auditing system to capture logins, attempted logins, log outs, administrative activities, and perhaps attempts to access or delete critical system files. Auditing should be limited to gathering just the information that is needed, as it does require CPU and disk time for auditing to gather information. It is encouraged that administrators also use the Solar Winds Log Management Software provided by ITS.

6. Mac Specific Security Best Practices

6.1 User Accounts

6.1.1 Securing Local Server Accounts

Unless administrator access is required, you should always log in as a non- administrator user. You should log out of the administrator account when you are not using the computer as an administrator. Note: The guest account is disabled by default. If you enable the guest account, enable parental controls to limit what the user can do and disable guest account access to shared files and folders by deselecting the "Allow guest to connect to shared folders" checkbox. The guest account should be disabled on all servers unless expressly needed for a specific purpose.

6.1.1.1 General Guidelines for Securing Accounts

Never create accounts that are shared by several users. Each user should have a personal standard or managed account. User authorization can be managed through a rights dictionary; however, this is probably not necessary for server administration.

Each user needing administrator access should have an individual administrator account in addition to a standard or managed account. Administrator users should only use their administrator accounts for administrative purposes.

When creating non-administrator accounts, you should restrict the accounts so that they can only use what is operationally required.

Accounts with administrator privileges should be used for login, and then the sudo command should be used to perform actions as root. Note: By default, sudo is enabled for all administrator users. You can disable root login or restrict the use of sudo command in the /etc/sudoers file. For more information, see the sudoers man pages.

To restrict sudo usage:

1. Edit the /etc/sudoers file as the root user using the visudo tool.
    a. $sudo visudo
2. Enter the administrator password when prompted.
3. Remove the line that begins with %admin, and add the following entry for each user:
    a. user ALL=(ALL) ALL
    b. Substitute the user's short name for the word user.
4. Save and quit visudo.

6.1.2 Disable the Root User

The root user is disabled by default.

Open Directory Utility, located in /System/Library/Core Services

Click the lock to make changes, and then enter an administrator name and password. Choose Edit > Disable Root User.

You can also disable the root account by using an administrative account and the dsenableroot command.

```
$ dsenableroot -d
```

6.2 Password Policy

6.2.1 Setting Global Password Policies

To configure a password policy that can apply globally or to individual users, use the pwpolicy command-line tool. You can set specific rules governing the size and complexity of acceptable passwords. For advanced password policies, use Password Server in Mac OS X Server.

You can use pwpolicy to set a password policy that meets your organization's password standards. For more information about how to use pwpolicy, enter man pwpolicy in a Terminal window.

Use logcheck for diradmin user when Open Directory is used:

For information on configuring logcheck refer to:
http://www.hmug.org/UnixHowTos/index.php?logcheck

6.2.2 Use Password Assistant

Mac OS X Server includes Password Assistant (PA), an application that analyzes the complexity of a password, or generates a complex password for you. You can specify the length and type of password you'd like to generate. You can choose from the following types of passwords:

- Manual: You enter a password and then PA gives you the quality level of your password. If the quality level is low, PA gives tips for increasing the quality level.
- Memorable: According to your password length requirements, PA generates a list of memorable passwords in the Suggestion menu.
- Letters & Numbers: According to your password length requirements, PA generates a list of passwords with a combination of letters and numbers.

- Numbers Only: According to your password length requirements, PA generates a list of passwords containing only numbers.
- Random: According to your password length requirements, PA generates a list of passwords containing random characters.
- FIPS-181 compliant: According to your password length requirements, Password Assistant generates a password that is FIPS-181 compliant (which includes mixed upper and lowercase, punctuation, and numbers).

6.2.3 Secure the Login Keychain

By creating a login keychain password that is different from the normal login password, your keychain will not be automatically unlocked at login. You can use Password Assistant to help you create a more secure password.

1. Open Keychain Access.
2. If you do not see a list of keychains, click Show Keychains. 3. Select the login keychain.
3. Choose Edit > Change Password for Keychain "login."
4. Enter the current password, and create and verify a new password for the login key chain.
5. Choose Edit > Change Settings for Keychain "login."
6. Select "Lock when sleeping."

6.3 Disabling Unused Services

6.3.1 Services Security

6.3.1.1 Managing Server Admin Utility

Disable any unused or unnecessary services using Server Admin.

Mail

- If running a mail server, deactivate unnecessary mail protocols. Use SSL certificates when possible to encrypt email transmission.
- Optional, enable SpamAssasin for filtering junk mail. Optional, enable CLAM for virus filtering.
- Optional, customize SMTP Banner in /etc/postfix/main.cf

File services

- Permissions should be carefully restricted for shared files/folders.
- Disable AFP, FTP, NFS, and Windows unless needed.

Web

Disable any unused web modules. Disable web server options that are not specifically required. For each site served set appropriate web access realms. Secure WebDAV and Weblog with SSL when in use.

- Use SSL for authentication when KSU NetIDs are involved.
- Use SSL for data encryption when KSU secure data is involved. Generate a key pair.
- Use a strong passphrase. Create a Certificate Signing Request (CSR) for the new key. Obtain a certificate from a CA.
- Use Server Admin to import and organize certificates.

Network Services

- Disable unused Network services like DHCP, DNS, and NAT.
- Optionally, unload Apple's Bonjour service, use the following command:
    - launchctl unload -w /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist
- Replace unload with load to restart Bonjour

6.3.1.2 Configuring the Application Firewall

Follow these steps:

1. Choose System Preferences from the Apple menu
2. Click Security & Privacy
3. Click the Firewall tab
4. Choose Turn On Firewall
5. Click Firewall Options
6. You can click on the “+” button to add an application to this list. You can select an application and click the “-“ button to remove it. Control- clicking on the application name gives you the option to reveal the application’s location in Finder.

Once you’ve added an application to the list, you can choose whether to allow or deny incoming connections for that application. You can even add command line application to this list.

When you add an application to this list, Mac OS X digitally signs the application (if it has not been signed already). If the application is later modified, you will be prompted to allow or deny incoming network connections to it. Most applications do not modify themselves, and this is a safety feature that notifies you of the change.

6.3.1.3 Security for Services Outside of Server Admin

Remote Access

- Use SSH to secure Apple's Remote Desktop communications.
- Disable ARD when it is not expected to be used.

Xgrid

- Password protect any agents that are grid enabled
- Specify controllers by IP or FQDN rather than browsing for them.

SSH

- Use /etc/ssh_known_hosts to limit user's outgoing SSH connections. Create a secure tunnel when an insecure network may be involved.

Energy Saver

- As this document is regarding servers, the energy saver settings are mostly moot. The server should be set to restart after a power failure. The screen saver should be set with a short inactivity interval. The screen saver should be password protected.

Expose, Spaces and Dashboard

- Avoid third party widgets or consider disabling dashboard with the two terminal commands below:
    - $ defaults write com.apple.dashboard mcx-disabled -boolean YES
    - KillAll dock
- You can restrict users from editing widgets and any preference

iCloud

- Do not enable iCloud for admin or root accounts.

Appearance

- It is best to set the number of recent items to none.

Bluetooth

- Set Bluetooth to off.
- Also, disable allowing Bluetooth devices to wake computer.

CD & DVD

- Choose Ignore for automatic actions with new media.

Network

- Set IP version 6 to Local-Link only. Automatic by default.

Print & Fax

- Do not allow servers to receive faxes.

QuickTime

- Except when necessary, do not install third-party QuickTime software.

Sharing

- Activating Remote Login will enable SSH for users.
- Apple Remote Desktop can be enabled.
- Make sure to logout of the server when done using ARD.

Sound

- For internal microphone, set "input volume" to zero
- For Line in, set "input volume" to zero

Security

- Require password to wake from sleep or screen saver
- Disable mouse and keyboard when Xserve is locked

1. Open System Preferences
2. Choose Security

Speech

- Do not enable speech recognition or speakable items for servers.

Spotlight

- Remove categories that should not be spotlight searchable by the users. The mdutil function can be used to remove entire volumes from Spotlight.
- By default, when the server app is installed, Spotlight is turned off.

- $ mdutil -E -i off volumename

Startup Disk

- Startup disks for servers should reside local/internal to the server.
- Avoid network volumes and target disks modes for a startup disk.

Time Machine

- Physically secure removable backup drives

6.4 System Security

6.4.1 Manage System Preferences

Users & Groups Manager

- Do not enable the Automatic login.
- It is best not to display a list of users in the login window. Remove unnecessary, old, or unused accounts.
- By default, users can only access their own account. Provide only the necessary administrative level for each user.
- Set Home and Disk quota limit when necessary.
- Enable Mail, Print, and Windows Access only when necessary.
- Besides the root and initial admin account, you should consider having more than one administrative access account. (Even if the secondary account is never or rarely used.)

Date & Time

- Correct time can be critical for some protocols like Kerberos
- The default NTP server is set for time.apple.com
- One can set NTP to a local and trusted time server

- Check Time Zone setting

Desktop & Screen Saver

- The screen saver should be set with a short inactivity interval.
- The screen saver should be password protected.
- Consider using the "Hot Corners" for quick activation.

6.4.2 Configure Access Warnings

To create a login window access warning:

1. Open Terminal.
2. Change your login window access warning:
    a. $ sudo defaults write /Library/Preferences/com.apple.loginwindow LoginwindowText "Warning Text"
    b. Replace Warning Text with your access warning text.
    c. Your logged-in account needs to be able to use sudo to perform a defaults write.

To create a command-line access warning:

1. Open Terminal.
2. Open /etc/motd in a text editor:
    a. $ sudo vi /etc/motd
3. Replace any existing text with your access warning text.
4. Save your changes and exit the text editor.

7. References

More detail about server security is available directly from Apple at: https://help.apple.com/advancedserveradmin/mac/3.0/#apd83039B4A-6BD7-44B3-BCA5-C4CDB4542D57

Apple Support: http://support.apple.com/