Baseline Server Configuration and Hardening Guidelines

1. Introduction

This document serves as a reference for systems administrators and IT support staff to ensure that server configuration guidelines are met. The configuration and hardening steps are not exhaustive and represent a minimum baseline for campus servers attached to the SF State network. Completion of these guidelines represents the initial stage of server administration, and should be incorporated into a comprehensive process including security reviews, ongoing maintenance, and other tasks. For those servers deemed to have a production role, this baseline configuration will be documented electronically and stored as a record to facilitate timely reviews by the ITS Security Team at a future date.

2. Scope

The outlined steps are platform neutral, and should be applied to all servers. Any exceptions to these requirements should be documented. Any server, including those with production, development, or test roles should follow the checklists outlined below.

3. Baseline configuration

A. Checklist for a Virtual Machine (VM) or Physical Server:

- Assign an IP address and register a DNS record
- IP address should reside on a separate subnet dedicated to servers
- Install the operating system
- Setup a local administrator account
- Update the operating system
- If desired, join to central campus Active Directory
- Install and configure necessary applications
- Setup remote access if necessary and use appropriate access controls
- Allow only appropriate users the permission to perform server administration
- Allow only appropriate users the permission to perform application administration
- Ensure system time and date are accurate, and setup timekeeping synchronization
- Configure log collection and set a retention window

- Configure log forwarding for those servers which permit user authentication via campus AD or shibboleth
- If necessary, configure automatic periodic backups
- Configure monitoring of the host, and if applicable, essential services. Alerts should be sent to appropriate administrators and/or stakeholders.
- Perform testing of the services and/or application.
- Document any necessary configuration parameters, application guidelines, or user support instructions.
- Facilitate any training or knowledge transfer to those users who will administer or support the server/application.
- Gain necessary approval to make production services available to the campus community/public internet if warranted.
- Communicate the launch of the service or application to appropriate entities.

B. Additional checklist for a physical server
   - Perform BIOS configuration and upgrade
   - Setup RAID (if applicable)
   - Setup out-of-band management (i.e. HP iLO or Dell DRAC)
   - Perform firmware and driver upgrades
   - Configure boot menu/order

4. Hardening checklist

- Configure automatic updates (via GPO or WSUS) and apply critical security fixes and essential application updates.
- Confirm that security updates are installed on a regular basis.
- If required, install anti-virus software.
- Remove or disable any services which are not necessary for the server/application to function properly.
- Remove or disable any user accounts which are not necessary for the server/application to function properly.
- Configure a host-based firewall, and where appropriate, allow necessary services access. Block access to unnecessary ports/services
- Secure the installed services which are exposed to the public internet, or the campus network.
- Setup a periodic Qualys scan, review the findings, and remediate vulnerabilities.

- Use the Qualys SSLLABS scan on publicly-facing websites and implement their recommendations if possible.