California State University Northridge
Information Security

CSUN Server Security Guidelines
September 20, 2006
DRAFT

Overview

California State University Northridge (CSUN) servers, networks, and the information that resides on them are critical assets for the university. These critical assets need to be protected to ensure their availability, confidentiality, and integrity. This document is intended to provide a set of guidelines for the installation of servers that are part of the CSUN network so that they meet a minimally acceptable level of security. For every operating system, it is important to follow the general guidelines below. The actual details used to implement these guidelines may vary, but the concepts are the same regardless of the operating system.

Guidelines

Before you connect the server to the CSUN network for the first time or upgrade to a new operating system, please review the following steps:

Review the purpose or the role of the server

1. Determine the purpose or role the server will play within the organization

Will the server act as a...

   a. Database repository (Oracle, MySQL, MS-SQL)
   b. Application server (WebLogic, Apache Tomcat, etc)
   c. Web server (Apache HTTP, IIS)
   d. File server
   e. Host for a shared business application

1. The services the server provides should entirely be dictated by its role within the organization and by the type of information (i.e., protected vs. "public") that flows through it
2. When setting up the operating system (OS), look for specific OS configuration options that will enhance the security of the server in this role
3. Ensure that the latest campus-supported stable version of the operating system is running
   a. Refer to the Operating Systems Guidelines document for information on the latest campus-supported stable version of operating systems
4. Harden the operating system (Windows, Unix, MAC OS, etc.)
   a. Eliminate unnecessary services, applications, protocols, and ports
5. Harden each application (Apache HTTP,IIS, MS-SQL, etc)
   a. Eliminate unnecessary services, drivers, protocols, and ports

Determine authentication requirements

1. Use the campus identity management system
    a. CSUN has established a campus identity management system, a unified directory service and authentication infrastructure. It is intended to provide campus departments with a centralized means by which departments can validate users who need or wish to access departmental applications, as well as to obtain authoritative information about users. The infrastructure can be used by applications for public directory service, lookups, authorization, and authentication.
2. All accounts should have strong passwords
3. Local accounts (as opposed to accounts from Active Directory) are strongly discouraged due to the difficulty of managing such accounts centrally
4. Assign a unique administrative account and unique password to each individual to better distinguish activities between multiple administrators
    a. While shared accounts are generally not allowed, some specific software programs require that such an account exist

        i. Obtain authorization for all exceptions and document them
        ii. Create inventory of any such created accounts and each user that has access it
5. Disable or rename the default administrator accounts
6. Require authentication for access by individuals to the server
7. Require re-authentication by users after idle periods

Secure access control

1. Restrict the number of accounts and privileges to only those who need access to perform their job function
    a. Give each user the minimum required amount of access to perform their work
2. Disable or delete old or unused accounts that belong to people who no longer need access
3. Regularly review the access list or log for users, especially of root and groups
    a. Look for unexpected rights or changes
4. Be sure to have a plan and process for securing administrator and root passwords that allows appropriate access to the server in case of illness, turnover, or unforeseen circumstances

Install only required software and keep operating system current

1. Run software that is current. The operating system and other installed software should be supported for the latest security patches
2. When installing software, make sure to only install software that is required, making sure to install the latest versions of all software including all recommended and security patches that are available.
3. Use the Automatic Updates feature of Windows (if running Windows) to keep the operating system patched
    - If Automatic Updates are not available or practical, download application patches to another computer and put on them on a CD or a network share that the server can access – never browse the web on a server, even for patches
4. After installation, all computers should be routinely maintained and updated
    - This includes the installation of operating system patches and new versions of installed software.

Run minimum number of services

1. Each computer should only provide services needed for its role or function in the organization
2. Make sure to configure all installed software, disable all unused features and be sure to limit the availability of any features that are enabled
    a. Any user not in the Administrators group should not have access to file-sharing unless the server specifically needs it
    b. If the server does not need to use email to send administrative-related messages, disable email related services
    c. If the server is not used to transmit data, disable file transfer related services
3. Use secure protocols (e.g. SSL/SSH/Kerberos) for accessing all servers and services that require and/or support authentication
    a. Disable Telnet and FTP – use SSH instead of telnet, and SCP instead of FTP
    b. Use RDP to connect to Windows servers – it is encrypted
4. Unless using network management tools, turn off SNMP. If SNMP is enabled, change the default community name and set permissions. Be sure to delete the public community string if the software allows you to do this, or at least change the default settings
5. Use of name services caching is okay, but do not run a name server

Install filters or firewall

1. Install and configure a packet filtering utility such as iptables or a host-based firewall to protect individual services
    a. The rules should reflect the acceptable use and security policies that have been defined for the computer
2. Operating system filters that deny or permit certain traffic should be used if available (e.g., most Unix and recent Windows versions)
3. Periodically review the filters for inappropriate or unneeded access
4. Restrict access to services to only CSUN IP addresses, where prudent
    a. Limit access to databases to specific static IP addresses or CSUN IP addresses.

Set up and review logs

1. Configure all services so that they log all connections and authentication information
    a. Forward all of these logs to a highly secure computer if possible
2. Enable local and domain auditing (if applicable) of security events
    a. Changes to user account and permissions
    b. Failed attempts to logon
    c. Failed attempt to access resources
    d. Changes to systems files
    e. Unsuccessful attempts to connect through the firewall
3. Someone should be assigned the responsibility of monitoring/reviewing and as appropriate following up on possible security violations identified in the system logs – typically these should be reviewed at a minimum on a monthly basis; weekly if possible
    a. For important servers this should be as often as daily

Install security related software

1. Install security related software on each computer, as appropriate to the level of security needed
2. Install anti-virus or other virus filtering software with daily updating for the latest virus definitions
3. Validate that antivirus definitions and engines are being updated
4. Run security analyzer software on servers, such as MSBA from Microsoft
5. SSH, RDP, or other encrypted and secure method of access should be installed if remote access or remote administration services are needed

    - SSH improves the security of user accounts by encrypting all login sessions and allowing the forwarding of X11 and other arbitrary network traffic

6. Install VPN encrypted tunnel if unable to install SSH or when clear text is a security risk

    - CSUN provides (free) VPN client software that provides an encrypted tunnel to the University from the Internet (e.g., connection at home or on the road)

Maintain physical security

1. Place the server in a secure location with documentation of who has physical access
2. Use Uninterruptible Power Supply (UPS) for servers and other essential peripheral equipment (e.g., monitors, KVM switches, etc.)
3. Locate servers in a climate-controlled environment (e.g., dedicated air conditioning with in-room temperature controls)
4. Consider basic fire suppression services/options (e.g., extinguishers, sprinklers, etc.)
5. Utilize "keyboard locking" software or password protected screen savers to prevent keyboard activity

Maintain backups and operational continuity

1. Run back-ups regularly and periodically store off-site
2. Test the restore capability periodically
3. Review backup history periodically
4. Use a "secure deletion" program to erase data from hard disks and media after done using and prior to transfer or disposal of hardware storing "protected" data
5. Develop business continuity plan for server

Identify the computer for security event notification

1. Identify critical servers by sending the name, IP address and contact information of responsible individual(s) to the Information Security department at security@csun.edu

Request a network-based vulnerability scan

1. Request a network-based vulnerability scan from CSUN Security to look for common vulnerabilities - these scans are highly recommended for important servers
    a. Send requests to security@csun.edu

2. Review and correct vulnerabilities found or implement a risk-mitigation strategy, concentrating first on the items marked as high

Where to go for help

If you have questions or concerns about the security of the data you store locally, on departmental, college, or university servers, please contact the Information Security department at extension 6100. The Information Security department can make arrangements for security tests to be run on critical servers or desktop machines to identify potential security risks. We can also schedule meetings with departmental IT personnel to talk with security analysts to help them improve the security of the systems they support.