Server Security Baseline Standard

1. Background

Before any server is deployed at the University of Cincinnati (UC), certain security baselines must be implemented to harden the security of the server. Servers that are not configured properly are vulnerable to hacking, malware, rootkits or botnet infection. Server administrators need to take steps to secure their systems against these types of malicious activities in order to protect the University's data and users. The steps outlined in this document are the minimum security measures that should be applied to any server. Additional steps would be required depending on the server function and the content residing on that server.

2. Audience

This policy applies to all organizations and individuals associated with UC who are responsible for the deployment of servers within the UC network.

3. Server Security Baseline

Most content adapted from NIST SP 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations and NIST 800-123 Guide to General Server Security.

The National Checklist Program (NCP), is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP can be utilized as an additional resource regarding security configurations of specific technologies.

3.1. Basic Security Steps

3.1.1. Plan the installation and deployment of the operating system (OS) and other components for the server, as discussed in Section 3.2.

3.1.2. Install, configure, and secure the underlying OS, as discussed in Section 3.3.

3.1.3. Install, configure, and secure the server software, as discussed in Section 3.4.

3.1.4. For servers that host content, such as Web servers (Web pages), database servers (databases), and directory servers (directories), ensure that the content is properly secured. This is highly dependent on the type of server and the type of content, so it is outside the

scope of this publication to provide recommendations for content security.

3.1.5. Employ appropriate network protection mechanisms (e.g., firewall, packet filtering router, and proxy). Choosing the mechanisms for a particular situation depends on several factors, including the location of the server's clients (e.g., Internet, internal, internal and remote access), the location of the server on the network, the types of services offered by the server, and the types of threats against the server. Accordingly, this publication does not present recommendations for selecting network protection mechanisms. NIST SP 800-41 Guidelines on Firewall and Firewall Policy and NIST 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS), contain additional information on network protection mechanisms.

3.1.6. Employ secure administration and maintenance processes, including application of patches and upgrades, monitoring of logs, backups of data and OS, and periodic security testing.

3.2. Installation and Deployment Planning

3.2.1. General Server Considerations

During the planning stages of server and system deployment, it is critical to consider security from the beginning. The following items are important to consider, and will make the process of employing security controls more efficient:

3.2.1.1. Identify the purpose(s) of the server.

3.2.1.2. Identify the network services and protocols that will be provided on the server. Some examples include HTTP, FTP, SMTP, NFS, and TCP/IP.

3.2.1.3. Identify any network service software, both client and server to be installed on the server and any other support servers.

3.2.1.4. Identify the users or categories of users of the server and any support hosts.

3.2.1.5. Determine the privileges that each category of user will have on the server and support hosts.

3.2.1.6. Determine how the server will be managed (e.g., locally, remotely from the internal network, remotely from external networks).

3.2.1.7. Decide if and how users will be authenticated and how authentication data will be protected.

3.2.1.8. Determine how appropriate access to information resources will be enforced.

3.2.1.9. Determine which server applications meet the organization's requirements. Consider servers that may offer greater security, albeit with less functionality in some instances.

3.2.1.10. Work closely with manufacturer(s) in the planning stage.

3.2.2. Operating System Considerations

Often the choice of server application may determine the server OS choice, however in general an OS should be selected that provides:

3.2.2.1. Ability to granularly restrict administrative or root level activities to authorized users only.
3.2.2.2. Ability to granularly control access to data on the server.
3.2.2.3. Ability to disable unnecessary network services that may be built into the OS or server software.
3.2.2.4. Ability to control access to various forms of executable programs, such as Common Gateway Interface (CGI) scripts and server plug-ins for Web servers, if applicable.
3.2.2.5. Ability to log appropriate server activities to detect intrusions and attempted intrusions.
3.2.2.6. Provision of a host-based firewall capability to restrict both incoming and outgoing traffic.
3.2.2.7. Support for strong authentication protocols and encryption algorithms.

3.2.3. Physical Location Considerations

Considering the location of the server is also very important for security. Due to the sensitive data that they may contain, it is critical that the servers are located in secure physical environments. When planning for this location, consider the following:

3.2.3.1. Appropriate physical security protection mechanisms for the server and its networking components, including locks, card reader access, security guards, and physical intrusion detection systems (e.g., motion sensors, cameras).
3.2.3.2. Appropriate environmental controls so that the necessary humidity and temperature are maintained, and the possible need for redundant controls.
3.2.3.3. Backup power sources and how long power can be provided.
3.2.3.4. Appropriate fire containment equipment that will minimize damage to equipment that would not otherwise be impacted by the fire.
3.2.3.5. Redundant network connections and redundant data center locations for high availability systems.
3.2.3.6. Protection from potential natural disasters that may exist in the server location.

3.3. Server Operating System Security

Many security issues can be avoided if the underlying OS on a server is

configured appropriately. Although the specific techniques for securing different OSs vary greatly, this guide includes procedures that are applicable to most common systems.

3.3.1. Patch and Upgrade Operating System

After OS installation, the following items are important to adequately detect and correct vulnerabilities that may exist on an installed server OS:

3.3.1.1. Create, document, and implement a patching process.
3.3.1.2. Identify vulnerabilities and applicable patches.
3.3.1.3. Mitigate vulnerabilities temporarily if needed and if feasible until patches are available, tested, and installed.
3.3.1.4. Install permanent fixes (patches, upgrades, etc.).
3.3.1.5. New or unpatched servers should be protected during the patching process. The following steps should be taken when preparing a server for deployment:
3.3.1.6. Keep the servers disconnected from networks or connect them only to an isolated "build" network until all patches have been transferred to the servers through out-of-band means (e.g., CDs) and installed, and the other configuration steps listed in this section have been performed.
3.3.1.7. Place the servers on a virtual local area network (VLAN) 16 or other network segment that severely restricts what actions the hosts on it can perform and what communications can reach the hosts - only allowing those events that are necessary for patching and configuring the hosts. Do not transfer the hosts to regular network segments until all the configuration steps listed in this section have been performed.

3.3.2. Hardening and Securely Configuring the OS

3.3.2.1. Remove or disable unnecessary services, applications, and network protocols

The following provide some examples of what services, applications, and protocols can be removed/disabled if they are not being utilized:

3.3.2.1.1. File and printer sharing services (e.g., Windows Network Basic Input/Output System [NetBIOS] file and printer sharing, Network File System [NFS], FTP).
3.3.2.1.2. Wireless networking services.
3.3.2.1.3. Remote control and remote access programs, particularly those that do not strongly encrypt

their communications (e.g., Telnet).

3.3.2.1.4. Directory services (e.g., Lightweight Directory Access Protocol [LDAP], Network Information System [NIS]).

3.3.2.1.5. Web servers and services.

3.3.2.1.6. Email services (e.g., SMTP).

3.3.2.1.7. Language compilers and libraries.

3.3.2.1.8. System development tools.

3.3.2.1.9. System and network management tools and utilities, including Simple Network Management Protocol (SNMP).

Completely removing unnecessary services is preferable to simply disabling them. It can enhance the security of the server in the following ways:

3.3.2.1.10. Other services cannot be compromised and used to attack the host or impair the services of the server. Each service added to a host increases the risk of compromise for that host because each service is another possible avenue of access for an attacker. Less is more secure in this case.

3.3.2.1.11. Other services may have defects or may be incompatible with the server itself. By removing or disabling them, they should not affect the server and should potentially improve its availability.

3.3.2.1.12. The host can be configured to better suit the requirements of the particular service. Different services might require different hardware and software configurations, which could lead to unnecessary vulnerabilities or negatively affect performance.

3.3.2.1.13. By reducing services, the number of logs and log entries is reduced; therefore, detecting unexpected behavior becomes easier.

3.3.2.2. Configure OS User Authentication

The following steps are recommended to ensure that appropriate user authentication is in place:

3.3.2.2.1. Remove or Disable Unneeded Default Accounts - The default configuration of the OS often includes guest accounts (with and without passwords), administrator or root level accounts, and accounts associated with local and network services. The names and

passwords for those accounts are well known. Remove (whenever possible) or disable unnecessary accounts to eliminate their use by attackers, including guest accounts on computers containing sensitive information. For default accounts that need to be retained, including guest accounts, severely restrict access to the accounts, including changing the names (where possible and particularly for administrator or root level accounts) and passwords to be consistent with the password policy.

3.3.2.2.2. Disable Non-Interactive Accounts - Disable accounts (and the associated passwords) that need to exist but do not require an interactive login. For Unix systems, disable the login shell or provide a login shell with NULL functionality (e.g., /bin/false).

3.3.2.2.3. Create the User Groups - Assign users to the appropriate groups. Then assign rights to the groups. This approach is preferable to assigning rights to individuals, which becomes unwieldy with large numbers of users.

3.3.2.2.4. Create the User Accounts - The deployment plan identifies who will be authorized to use each computer and its services. Create only the necessary accounts. Permit the use of shared accounts only when no viable alternatives exist. Have ordinary user accounts for server administrators that are also users of the server.

3.3.2.2.5. Configure Automated Time Synchronization - Some authentication protocols, such as Kerberos, will not function if the time differential between the client host and the authenticating server is significant, so servers using such protocols should be configured to automatically synchronize system time with a reliable time server. Typically the time server is internal to the organization and uses the Network Time Protocol (NTP) for synchronization; publicly available NTP servers are also available on the Internet.

3.3.2.2.6. Check the Password Policy - Set account passwords appropriately, according to the details outlined in the policy.

3.3.2.2.7. Configure Computers to Prevent Password Guessing - If provided by the OS, configure the computer to increase the period between login attempts with each unsuccessful attempt. An

alternative would be denying login for a period of time after a set number of failed attempts.

3.3.3. Install Additional Security Controls

OS's often do not include all necessary security controls to adequately protect a server system. In these situations, administrators may need to utilize additional software to provide these controls. The following list provides some examples Anti-malware software, including antivirus software, anti-spyware software, and rootkit detectors.

3.3.3.1. Host-based intrusion detection and prevention software (IDPS).
3.3.3.2. Host-based firewalls.
3.3.3.3. Patch management or vulnerability management software.
3.3.3.4. Disk encryption technologies.

3.4. Server Software Security

After the operating system has been installed, configured, and secured, the necessary server software must be installed. Security principles also must be applied to the configuration of this software.

3.4.1. Securely Installing Software

The following steps should be performed when installing the server software on the system:

3.4.1.1. Install the server software either on a dedicated host or on a dedicated guest OS if virtualization is being employed.
3.4.1.2. Apply any patches or upgrades to correct for known vulnerabilities in the server software.
3.4.1.3. Create a dedicated physical disk or logical partition (separate from OS and server application) for server data, if applicable.
3.4.1.4. Remove or disable all services installed by the server application but not required (e.g., gopher, FTP, HTTP, remote administration).
3.4.1.5. Remove or disable all unneeded default user accounts created by the server installation.
3.4.1.6. Remove all manufacturers' documentation from the server.
3.4.1.7. Remove all example or test files from the server, including sample content, scripts, and executable code.
3.4.1.8. Remove all unneeded compilers.
3.4.1.9. Apply the appropriate security template or hardening script to the server.

3.4.1.10. For external-facing servers, reconfigure service banners not to report the server and OS type and version, if possible.
3.4.1.11. Configure warning banners for all services that support such banners.
3.4.1.12. Configure each network service to listen for client connections on only the necessary TCP and UDP ports, if possible.

3.4.2. Configuring Software Access Controls

The typical files to which access should be controlled are as follows:

3.4.2.1. Application software and configuration files.
3.4.2.2. Files related directly to security mechanisms, including password hash files.
3.4.2.3. Server log and audit files.
3.4.2.4. System software and configuration files.
3.4.2.5. Server content files.

It is also important to limit the files which can be accessed by the service processes. The following should be enforced with access controls:

3.4.2.6. Service processes are configured to run as a user with a strictly limited set of privileges (i.e., not running as root, administrator, or equivalent).
3.4.2.7. Service processes can only write to server content files and directories if necessary.
3.4.2.8. Temporary files created by the server software are restricted to a specified and appropriately protected subdirectory (if possible). Access to these temporary files is limited to the server processes that created the files (if possible).

3.4.3. Configuring Server Resource Constraints

In order to mitigate potential effects of certain DoS attacks, the server should be configured to limit the amount of OS resources consumed. This can include the following:
3.4.3.1. Installing server content on a different hard drive or logical partition than the OS and server software.
3.4.3.2. Placing limits on the amount of hard drive space dedicated for uploads, if uploads are allowed to the server. Uploads should also be placed on a separate partition if possible.
3.4.3.3. Ensure that files uploaded to the server are not readable by the server until some process is used to screen them, preventing malware or attack tools.
3.4.3.4. Configuring the maximum number of server processes

and/or network connections that should be allowed on the server.

4. Related links

Security Standards
Data Governance & Classification Policy
Vulnerable Electronic Systems Policy
Acceptabe Use of University Information Technology Resources Policy

5. Contacts Information

IT@UC Office of Information Security 513-558-ISEC (4732) Email: infosec@uc.edu

History
Effective Date: 3/15/2015
Revised Date: 3/31/2017