Server Hardening

The University of Waikato

Title	Server Hardening
Author	Milton Markose (Systems Administrator – Security)
Contributors	Information Security Forum (ISF)
Date	21-08-2014
Reviewed By	Information Security Forum (ISF)
Document Version	Final V1.0

Revision History

0.1 (draft)	09/12/2013	Initial Server Hardening doc	Milton Markose
0.2 (draft)	01/04/2014	Updated and shared with ISF Members	Dougal Mair
0.3 (draft)	22/07/2014	Amendments following review by ISF	Dougal Mair
1.0 (final)	21/08/2014	Approved by ICT Committee	Dougal Mair

Table of Contents

Purpose

The purpose of this server security hardening standard is to attain a much more secure server operating environment in the University of Waikato. To protect our servers, we have established best practices and policies for hardening the server operating systems. This server hardening document explains how to deploy a server in the most secure state possible by reducing as many threat vectors as possible while maintaining the server's functionality.

Scope

The Server Hardening process document applies to all University servers and should be followed when a new server is setup. These server hardening guidelines are intended to be the minimum protection that each server operating system should have. Some exceptions can be allowed based on the requirement and an understanding of the risk the exception may raise; such exceptions must be properly documented.

General Guidelines Applicable to All Servers

Operating System Version

We encourage the use of Enterprise focused operating systems.

When selecting the operating system version for a new server, the support lifecycle should be taken into consideration. Only under exceptional circumstances should an operating system version that is no longer in support, or for which support will end in the near future, be installed.

Pre-release or immature projects should also be avoided where possible.

Where applicable, the most recent service pack / service release should be used.

Patching

As part of the hardening process for a new server, the following should be installed:

- All security updates
- All firmware updates recommended by the vendor
- All non-security updates / hotfixes recommended by the vendor
- The latest available device driver versions recommended by the vendor
- The latest anti-virus software version and virus definitions (if applicable)

If any additional applications not included with the operating system are to be installed, they must also be updated in the same way.

Configuration

- A firewall should be installed, and should be configured to block incoming access by default. Only those exceptions that are necessary for the proper functioning of the server should be enabled.
- Unnecessary software components should not be installed / enabled.
- Each server should have a distinct local administrator /root password. This password should be stored in a secure way in case it is needed. *ITS Only:* the local administrator / root password must be saved in KeePass Password Safe.
- Access to the server must be properly restricted. Each form of access must be considered; for example, a file server might be configured to grant all users access to certain network shares, but interactive logon should be restricted to System Administrators only.

Steps Required Before Putting a Server into Production

- An internal vulnerability scan should be performed.
- All test data and accounts must be removed before production systems become active.
- All custom application accounts, usernames, and passwords must be removed prior to applications becoming active or being released to faculties.
- A peer review must be performed to confirm that the requirements of this document have been met.

Guidelines Applicable to Windows Servers

General

- The Symantec Endpoint Protection (SEP) client should be installed on all Windows servers.
- Older file systems such as FAT, FAT32, etc., which do not support file-level security and auditing, must not be used.
- The guest account must be disabled (unless required).
- No unnecessary file shares should be configured.
- Do not enable any unwanted services.
- As part of the initial patching process, and again before being put into production, Windows Servers should be scanned against Windows Update or Microsoft Update as well as against the appropriate WSUS server.

Virtual Server Templates

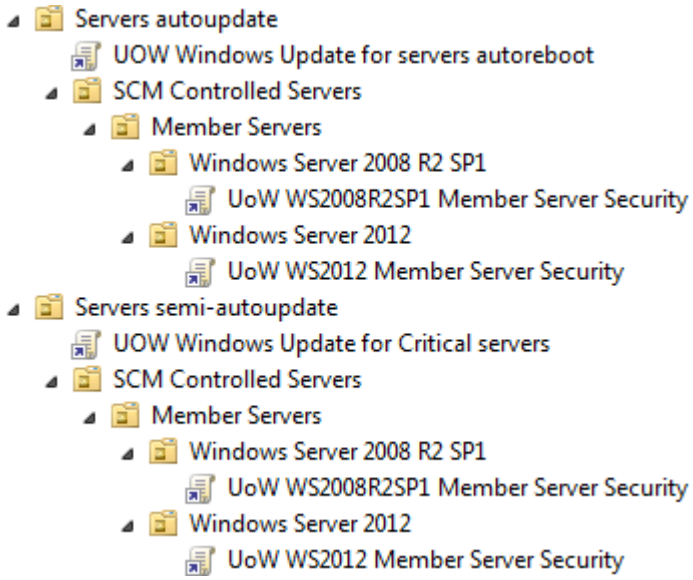
To simplify virtual server deployment, ITS maintains templates for all versions of Windows commonly used in the University. In most cases, faculty requests to the Systems Team will be for a new blank Virtual Server (without any OS) or for a new Virtual server based on the existing templates. In either case, the Systems Administrators or Systems Owner of the new server is responsible for ensuring that the deployment conforms to the Server Hardening standards.

These templates are maintained by the ITS Systems Team and will be configured in accordance with the Server Hardening standards:

- They will have the latest service packs installed and be kept reasonably current with post-service pack updates.
- They will have the Symantec Endpoint Protection (SEP) client installed and be kept reasonably current with anti-virus definitions.
- They will have the guest account disabled.
- They will have no non-administrative file shares configured.
- The Windows Firewall will be enabled with no unnecessary exceptions configured.
- They are configured with defined disk size(s).
- They are configured by default with isolated network settings.

GPO based Windows Server hardening

The University of Waikato recommends that all Windows based servers make use of the GPO settings created and maintained by ITS Infrastructure team. These security GPOs are created using the Security Compliance Manager (SCM) tool which brings together Microsoft's best practices around security settings.



Changes to these GPOs will only be made following consultation with the ISF, and will follow the change management process.

Guidelines Applicable to Linux Servers

General

- *ITS Only:* all critical systems logs should be saved to SCARAB.
- *ITS Only:* the standard repository must be configured to fetch packages from SCARAB.

ITS Puppet server (ITS servers only)

The ITS Systems Team uses Puppet Server to setup and configure new ITS Linux servers. Two instances of puppet servers are running to form a Puppet cluster system. ITS has the standard repository created on SCARAB (the Systems Team's Operations server) for all the ITS Linux servers and the repository is updated every night.

Puppet modules are configured to ensure that:

- Specified users are allowed to access the server with the right permissions and all other user access is blocked.
- Unwanted services are stopped and disabled.
- Only required packages are installed.
- Nagios is configured for monitoring purposes.
- The Networker client is installed where required.
- The standard repository configuration is used.
- IPTABLEs are configured with only those rules that are required to communicate.

Virtual Server Templates

To simplify virtual server deployment, ITS maintains templates for certain versions of Linux that are in common use in the virtual environment. In most cases, faculty requests to the Systems Team will be for a new blank Virtual Server (without any OS) or for a new Virtual server based on the existing templates. In either case, the Systems Administrators or Systems Owner of the new server is responsible for ensuring that the deployment conforms to the Server Hardening standards.

These templates are maintained by the ITS Systems Team and will be configured in accordance with the Server Hardening standards:

- They will be kept reasonably up to date with the latest patches.
- Unwanted services will be stopped and disabled.
- Only required packages will be installed.
- IPTABLEs will be configured with only those rules that are required to communicate.
- They are configured with defined disk size(s).

Firewall

Once the server is ready, it should be configured within the University's firewall with policy appropriate to the server's role. A LANDesk request should be sent to the Networks Team with the list of ports to be opened for the server.

Please note - configuring the firewall is not as straightforward as opening ports externally (i.e. to the Internet and REANNZ network). Due to internal virtual security domains (VDOMs) there are policies required for internal networks as well (e.g. eduroam, the VPN link to Tauranga, etc). If System Administrators are unsure of what firewall configuration changes they need for a new server they should consult with the ITS Networks Team.

Preferably, an internal vulnerability scan should be performed (and all issues addressed) before requesting any firewall changes.

Vulnerability testing

All servers should undergo a vetting process that includes external and internal vulnerability scanning. All vulnerabilities should be addressed before the server goes into the production environment.

Internal vulnerability scan

The internal vulnerability assessment of a server should be done using the ITS Infrastructure Team's FortiAnalyzer system. The scan should be an authenticated one with a 'Full scan' option. A LANDesk request should be sent to the ITS Systems Team when ready for this scan to be completed.

External vulnerability scan

The University of Waikato uses OpenVAS scanning software to perform external scanning on servers. Thorough scanning will be done on a new server based on its operating system before the server goes 'live'.

Microsoft Baseline Security Analyzer

All Windows based servers should be tested using the Microsoft Baseline Security Analyzer tool to identify missing security updates and common security misconfigurations before they go to production.

On-going Server Hardening

As security vectors change, the security measures applied to servers will need ongoing assessment. Once servers are 'live', the steps below should be followed to ensure a secure environment.

- Periodic patching when updates are released by the vendors. This includes both the operating system and any installed applications, and is described in Patch Management - Servers and Services policy document.
- Scheduled internal and external scanning to identify any new vulnerabilities.

Roles and Responsibilities

- System Owners and System Administrators are responsible for ensuring that the deployment of servers is managed according to these standards.
- Oversight of System Owners and System Administrators, to ensure that these standards are followed consistently, is the responsibility of the relevant line manager(s) as well as the Dean, Head, or Chairperson. In the case of ITS, this responsibility is delegated to the System Administrator – Security.
- Additional oversight is provided by the ISF group.
- ITS is responsible for maintenance of the virtual machine templates.
- ITS is responsible for conducting vulnerability scanning.
- ITS is responsible for maintenance of the Windows server GPOs.

Definitions

- Service - IT functionality provided by software running on a server. Services may be provided by the server's operating system itself, or by a separate installed software package.
- Server - a physical or virtual computer providing one or more services.
- Update, Patch, Hotfix - a modification to or new version of software, typically correcting one or more faults in the software, improving performance, and/or adding new functionality.
- Upgrade - a new and significantly changed version of software. This is most often applicable to operating systems or major application packages. Upgrades generally take more work and are slower to install than updates, and require more extensive precautions such as an extended testing period.
- Service release or service pack - a release of software that bundles together several patches and/or updates to provide a clear benchmark or version level of release (e.g. Service Pack 1). Service packs typically take longer to install than individual updates, and require some additional testing, but not as much as upgrades.
- Device Driver - Software required by the operating system to make a piece of hardware function.
- ITS Only - as used in this document, "ITS Only" describes policy and procedures applicable to ITS.
- KeePass - KeePass Password Safe is a software password management utility.
- Nagios - an open source computer system monitor, network monitoring and infrastructure monitoring software application.

- Networker - a backup solution from EMC.
- Puppet - an open source configuration management tool.
- Firewall - a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or host.
- FortiAnalyzer - a network vulnerability scanner used by University to perform internal scanning.
- OpenVAS - a framework of several services and tools offering a vulnerability scanning and vulnerability management solution.
- GPO - Group Policy Object, used to change configuration settings on computers within a Windows Active Directory domain.