4.2.2 Hardening Facts

This lesson covers the following topics:

- Harden the system
- Manage updates

Harden the System

Hardening is the process of increasing the security of devices and software. You can harden a network and reduce your security exposure by tightening security controls. Improved performance may result from the hardening process, but it is not the primary goal.

The first step should always be to improve the security of the most foundational elements. You can harden specific hardware devices as well as the software running on the device. The following table describes recommendations for hardening systems.

Recommendation	Description
Use a Trusted Operating System (TOS)	A TOS is an operating system that comes hardened and validated to a specific security level as defined in the Common Criteria for Information Technology Security Evaluation (CC). Many TOSs provide sufficient support for *multilevel security*, a system in which multiple levels of classified data reside within the same system, but users are not permitted to access data at different classification levels. Additionally, all personnel must have access approval on a need-to-know basis.
Control login	To control login and access to a system, you can: - Limit privileges, especially administrative privileges. - Change default passwords - Require complex passwords - Require multi-factor authentication - Use smart cards, finger print readers, text services, or other apps that send verification codes

Use configuration baselines	A *configuration baseline* is a set of consistent requirements for a workstation or server. A *security baseline* is a component of the configuration baseline that ensures that all workstations and servers comply with the security goals of the organization. Use configuration baselines as follows:
	- Identify common configuration baselines that should be applied to all, or a group, of systems.
	- Use security templates to quickly apply security baseline settings. A *security template* is a saved set of configuration values that produce the system configuration as specified in the configuration baseline. When you apply the security template to a system, the settings within the template are applied to the system. Use security templates to:
	  - Quickly apply settings to one or more computers.
	  - Configure consistent security settings between devices.
	  - Quickly restore security settings to the baseline.
	- Compare the actual settings on a device to the settings required by the configuration baseline.

	Microsoft operating systems include the following tools for managing security templates: ▪ The Security Templates snap-in, which creates and edits templates. You can obtain security templates from various sources, including the NSA, which has predefined settings it believes are appropriate for Windows operating systems. ▪ The Security Configuration and Analysis snap-in, which compares the existing settings with the template or applies a template to a single device.. ▪ The Group Policy Editor, which imports a template into Group Policy and applies the template to multiple computers.

Manage software	Tips for managing software include:
	▪ Check that all software has up-to-date licenses. A license compliance violation may open your organization to legal actions and may cause a vital application to cease its functions.
	▪ Install security software such as anti-virus, anti-spyware, anti-rootkit, and firewall.
	▪ Install only needed software.
	▪ Avoid installing freeware or software from untrusted publishers.
	▪ Reduce the attack surface of the device by limiting applications and services running on the device and removing unnecessary software, features, and non-essential services.
	  ▪ Use role separation by installing services on separate physical systems. If a single system is compromised, only the few services on that system will be affected.
	  ▪ Remove unnecessary services, protocols, and applications following installation. Unnecessary services are often installed in new systems by default.
	  ▪ Determine the dependencies of services you are using before removing existing services.Examples of non-essential services are TFTP, Telnet, and SNMP. DNS, ICMP, and NNTP are generally considered essential protocols and services; however, consider the function of your system before leaving them on the system.

Use a Standard Operating Environment (SOE)	Most organizations maintain a Standard Operating Environment which is implemented as a standard disk image or master image. This disk image is used when deploying new computers to the network. Automation is used when deploying the master image and when running configuration scripts, to give the computer a name, to join a domain, and during any other customizations. The use of a master image and automation can reduces security risks by ensuring that security standards are consistent throughout the network. Master images should be based on a TOS and be fully patched.

Managing Updates

Keep the operating system and applications at the most current levels by applying updates. The following table describes the three types of updates

Update Type	Description

Hotfix	A *hotfix* is a quick fix for a problem. Normally, you install a hotfix only if you have the specific problem it is intended to fix. Hotfixes are: ▪ Typically made to address a specific customer situation and possibly may not be distributed outside that customer organization. ▪ Commonly used to address freshly discovered security holes.
Patch	A *patch* is also a quick fix, but generally more thoroughly tested than a hotfix and designed for a wider deployment. Patches: ▪ Include previous hotfixes that the manufacturer has thoroughly tested for mass deployment. ▪ Include fixes that should be applied to wider audiences, such as patching security holes. The best place to obtain updates is from the manufacturer's website.
Service pack (SP)	A *service pack* (SP) is a collection of patches, hotfixes, and other system enhancements that have been tested by the manufacturer for wide deployment. A service pack includes all previously released bug fixes. If you install the service pack, you do not need to install individual patches. Installing a service pack also includes all previous service packs.

You do not necessarily need to install every hotfix, patch, or service pack that is released. For example, if a hotfix applies to a service that you have disabled on your servers, applying that hotfix is not required. Or if a patch applies to browser security and the browser on the server is not used, you don't need to install the patch.

When using a patch, follow the recommendations in the following table::

Recommendation	Description
Use patch management activities	Patch management activities include: ▪ Determining the patches that are needed on the system. ▪ Testing patches in a lab environment to identify the effects of applying the fixes. ▪ Applying the patches. ▪ Auditing for successful application of patches.
Use patch management software	Use patch management software to simplify the patch distribution and management process. Windows Software Update Services (WSUS) is a patch management tool that allows clients on a network to download software updates from a WSUS server internal to their organization. ▪ The WSUS server receives a list of available updates from Microsoft. ▪ On the WSUS server, you identify allowed or required patches for your organization. ▪ Clients download only approved patches from an internal WSUS server or directly from Microsoft. You can also use Group Policy to distribute and automatically install patches. You must use Group Policy to install updates to non-Microsoft software that is not supported by WSUS.

Test patches	Be sure to test patches before applying patches within your organization. A common strategy is to: 1. Apply and test patches in a lab environment. 2. Deploy patches to a set of systems, such as a single department. 3. Deploy patches system-wide.

Copyright © 2022 TestOut Corporation All rights reserved.