Hardening

We can mitigate the risk by minimizing the vulnerabilities in an effort to reduce our exposure to threats, but we can't eliminate the risk completely. Risk can only be minimized because there's always some kind of threat and some kind of vulnerability in a given system.

Restricting Applications & Services

In our corporate networks, it's common for us to create a secure baseline image that we use for all of the work stations across the company. This image will have the operating system, the minimum applications required, and strict configuration policies that are set up for all of those machines.

We can use Microsoft's system center configuration management or the SCCM tool that allows us as admins to manage large amounts of software across the network, as well as push out new configurations and policy updates to all of our PCs.

With application whitelisting, only applications that are on the approved list are allowed to be run by the operating system. All the other applications are blocked from running.
With application blacklisting, any application that's placed on a list will be prevented from running, while all of the other applications will be permitted to run.

Using application whitelisting is much more secure, because everything is denied by default, and only the applications listed can actually run.

Windows Services

We're going to hit on the Windows key in the corner, the start menu, and we're going to type in services.msc and hit enter.

We can do this same thing inside the command prompt. To do that, just click on your Windows key and type command prompt, or CMD.

From here, you can use sc, which is to control it through the services, stop, and the name. For that program that we just stopped, it is the wuauserv, which is the name of the Windows Update program.

The other way you can stop this in Windows is using the net command. And it's net stop and the name of the service that you want to stop.

Mac OS X Services

To do that, you can go ahead and first we're going to create something to kill. So, I'm just going to create a Textpad, and I'm going to call it kill this process when ready, and that just gives me something that I'm going to be able to kill. Now, to find it, I'm going to go ahead and use the Activity Monitor, which is under your applications, then go to utilities, and then Activity Monitor. From here, I'm going to sort by process name and find TextEdit.

And if I want to get rid of this, all I have to do is quit. It's going to ask me if I want to quit it cleanly, like you normally would quit an application, or force quit it, which terminates it immediately.

Linux Services

I can use the command top. Top will show me what processes are currently running. Processes are also known as services.
In this case, it's the TextEdit, and the process ID is 2513. So, what I'm going to do is I'm going to quit. And to kill it, you just type in kill and the process ID, 2513, and watch on the right side as TextEdit goes away.

Trusted OS & Patches

What operating systems meet the criteria to be called a Trusted Operating System? Well, every version of Windows since Windows 7 is considered a Trusted Operating System. This includes Windows 8, Windows 10, Windows Server 2012, and Windows Server 2016. Also, every version of Mac OS X since version 10.6 is classified as a Trusted Operating System. If you're using FreeBSD, if you load the TrustedBSD extensions, this is also considered trusted, as well as Red Hat Enterprise Server.

For a Windows machine, you simply run the msinfo32.exe program from the Command Prompt and it'll display the exact version and build of the software.

Originally, a hotfix was different from a patch. A hotfix could be installed without requiring a reboot of your system. But a patch required a system reboot. Over time, patches and hotfixes began to be used interchangeably by most manufacturers. Today, whether you call it a patch or a hotfix, it really refers to the same thing.

Update Categories

1. First, we have a Security Update. Security updates are a type of software code that's specifically issued from a product-specific security-related vulnerability. So, if a hacker finds a bug in the code for Microsoft Word, that may allow them to breach your security. Microsoft would release a security update that contains a patch to correct the bug in the code.

2. The second type of update is a Critical Update. A critical update is a piece of software that's designed for a specific problem that addresses a critical, non-security bug in a piece of software.

3. A third type of update we have is a Service Pack. A service pack is actually a grouping of other patches. It contains hotfixes, security updates, critical updates, and possibly even some feature or design changes. Service packs are commonly seen with an operating system update.

4. The next type is called a Windows Update. This is a recommended update to fix a non-critical problem that certain users have found, and it may also provide some additional features or capabilities.

5. The final type of update is a Driver Update. Driver updates provide either a security fix or additional features for a supported piece of hardware.

Patch Management

There are four steps to patch management:

1. Planning
2. testing
3. implementing
4. auditing

Microsoft actually provides a useful tool that can help us in determining the status of our system, and whether or not a patch needs to be applied. This is known as the Microsoft Baseline Security Analyzer or MBSA.

Group Policies

A Group Policy is a set of rules or policies that can be applied to a set of users or computer accounts within an operating system. Now, to Access the Group Policy Editor, simply go to the run prompt and enter gpedit.

A large part of hardening the operating system occurs through loading different Group Policy objectives or GPOs against the workstation or against the server. These Group Policies are also used to create a secure baseline as part of your larger Configuration Management Program.

FS

We have things like:

1. NTFS
2. FAT32
3. ext4
4. Hierarchical File System Plus - HFS+
5. Apple File System.

FS Checks

If you're running Windows, you can do this by running Check Disc, and the System File Checker.

If you're using Linux, you should do a file system check by typing fsck in the terminal.

If you're using OS X, you can run first aid from within the disc utility application.