LESSON GUIDE

INTRO TO CYBERSECURITY

Securing the System

3.1.2 - Hardening Systems Part 1

Lesson Overview:

Students will:

- Identify host-based defensive tools to harden and restrict access.
- Apply a vulnerability assessment tool and use results to secure a system.

Guiding Question: How can we use defensive tools to harden and restrict access to better secure a system?

Suggested Grade Levels: 8 - 12

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Hardening Systems Part 1

Slide 1 - Intro Slide

Slide 2 - Vulnerabilities in Digital Products & Systems

We learned in the previous 2 lessons how every system has multiple vulnerabilities which can be used by hackers in their attacks. It is now time to learn about the best practices to harden a system to mitigate against these attacks.

Hardening limits potential weaknesses that make systems vulnerable to cyber-attacks. More secure than a standard image, hardened virtual machine images help protect against denial of service, unauthorized data access, and other syber threats.

Definition Source = https://www.cisecurity.org/insights/blog/5-tips-to-harden-your-os-on-prem-or-in-the-cloud

"Hardening a System" or "Sytem Hardening" are both terms the process of securing the host system through a series of configuration steps.

Benchmarks are a way of identifying secure configurations without having the expertise to research it yourself. From CIS website: *"CIS Benchmarks are recommended technical settings for operating systems, middleware and software applications, and network devices. Developed in a unique consensus-based process comprised of hundres of security professionals worldwide as de facto, best-practiced configuration standards…"*

Slide 3 - Which benchmarks? Scan to get advice

It is not possible to manually identify all the configuration changes needed to secure a system. A **vulnerability assessment tool** is used for this task. While there are hardening steps that are recommended for most systems, each device will have some differences form lots of reasons such as where it is being used or what applications are installed or how old. it is. Before trying to harden a system, it is a good idea to first perform a **vulnerability scan**.

Many organizations use the free CIS-CAT tool from the Center for Internet Security (CIS) which uses the CIS benchmark documents to provide a report on recommended changes.

The recommendations from the Scan are based on Microsoft or industry best practices. The IT administrator will run these scans regularly to identify any insecure configurations.

The lesson lab uses the older Microsoft Baseline Analyzer scan which will do a less complete scan but does give effective recommendations on key configuration settings.

Slide 4 - Steps to Harden a System - Part 1

There is a lot to know about hardening a system, but in this slide, we have the "short list" (part 1) of what needs to be done. For this lesson, we are approaching this from the view of what an enterprise would do to harden their Windows 10 laptops and desktops. The security categories are pertinent to most operating systems even though the actual implementation steps would be different.

Slide 5 – Updates

Animated slide, bullets appear on click.

If a user is going to choose only ONE action to secure their system, then Updates should be it by a mile! Note that this applies to all devices smartphones, wifi routers, printer drivers - even the software in your car!

All updates are actually adjustments to the Operating System's original code, but there are. different categories depending on what the adjustment will accomplish.

Here is more detail as to the above definitions:

- A "regular" update (aka patch) is only intended to keep improving that Operating System version. But you can't opt out of these for too long because newer updates to code may rely on your OS having the previous tweaks. **With Windows 10, updates are now installed automatically by default, but users can turn off this feature or pause the update cycle.**

- A hotfix is only created to address a specific problem - for instance, the newest Lenovo laptop has a driver that causes Win10 Wifi to crash. Then only the owners of new Lenovos will need this hotfix update. That's why hotfixes are usually not publicly released on Automatic Updates. The users who need the hotfix need to find it online, download it and install it themselves.

- A critical update is issued when something significant is wrong with the OS code that affects whether it even works. These are very uncommon, usually seen with Beta or newly issued versions of an OS.

- A security update is the most common type of update. These address the newly found vulnerabilities in the OS and should be installed ASAP to avoid being exploited.

Slide 6 - Update Settings

1. In the Windows Search Box, type Update, click Enter and then from the results, select Windows Update Settings.

2. It is very common to see an error notice of some kind either because Automatic Updates was not turned on, or they were disconnected from the Internet. Also, many organizations will first test an update on a "non-production" device first then do a full rollout to all devices once the update is confirmed to not cause any glitches.

3. Notice that until updates are installed, this device is vulnerable because security fixes are missing. Users often don't realize they aren't current with updates because they have been disconnected from the Internet or haven't allowed the necessary restarts or perhaps used the Pause feature. THIS IS BAD!

Slide 7 - Windows Security

The easiest security procedures to implement are those that come built-in with the Windows OS. In Win7 it was called the Action Center and in Windows 10 it is called Windows Security. Regardless of the name, the security components are essentially the same - Virus & Threat Protection, Firewall & Network Protection, Apps & Browser Control. The Windows Operating System will provide alerts when these security components are not working or not configured properly.

Slide 8 - Users as a Vulnerability

Establish the point that users are a key vulnerability area for any system. There is a basic security problem – we want users to be able to use the system and apps BUT we must limit their actions in case they make incorrect decisions, or their account is taken over.

Since most computers are intended to have user interaction, this means that user access is one of our biggest vulnerabilities. A joke in Cybersecurity is that *the best way to secure your computer is to unplug it from power and the next best way is to not allow any users.*

Obviously, neither of those is a serious solution, so we will have to find different solutions to the user access problem. The first step is to ask the questions in this slide and make security adjustments based on the answers.

Slide 9 - UAC - User Access Control

UAC got a very bad reputation from its first implementation in Vista because it was to trigger happiness to restrict just about everything. But the UAC that exists in Win 7 and later is not only a better-designed tool, but you also could have the ability to set levels of control.

Often our computers are infected or breached because we, the users, click on a link or download a Trojan or go to a sketchy website - and when we do, malicious code will try to take some action on our computer. **UAC is our only hope that it will be stopped!**

Slide 10 - Local Security Policies

All Operating systems have methods of enforcing rules. The Windows "Local Security Policies" tool makes it possible to apply rules to some very important user interactions. We can force the user to have a strong password and reset it at regular intervals. We can make sure they don't reuse the same password. And if someone tries to brute force the password by trying to guess it, then we can lockout them out after a certain number of tries. (Yes, sometimes we lock out the real user, but they need to remember their password!)

Slide 11 - Local Policies

Besides enforcing passwords and blocking brute force attacks, there are many other ways that security policies can be used to protect the system.

In the example, the logs would show the username jsmith with multiple login attempts sequentially over a short time period. That means someone kept trying the same username with different passwords - i.e. a brute force attack.

But the number and complexity of the possible settings can make it very confusing, so this is where benchmarks become very useful.

Slide 12 - Services & Applications

The next item to investigate for hardening is what services are running on this computer. Services are built-in programs to make your computer "do" something - usually it's to provide a function or interaction with other computers.

Slide 13 - Remove Unneeded Services

There are dozens of services that are commonly turned on in systems. Here are some key questions to ask:

- Why is it here? Did it come by default? Did a user install it?
- Do I need it? What happens if I turn it off or uninstall it?
- Of the services I am keeping, what are their vulnerabilities? What can go wrong with those flaws?
- What are the best practices for securing that service?

Slide 14 - Lab: MBSA Vulnerability Scan

Lab: MBSA Vulnerability Scan - Examine how to perform an initial vulnerability assessment on Windows OS systems using the Microsoft Baseline Security Analyzer tool. An MBSA scan will identify missing security updates and common security misconfigurations for a Windows OS device.