LESSON GUIDE

INTRO TO CYBERSECURITY

Foundations and Threats

3.1.1 - System Vulnerabilities

Lesson Overview:

Students will:

- Define vulnerabilities.
- Identify commonly seen types of vulnerabilities.
- Examine how the Common Vulnerability and Exposure database can be used as a research tool.

Guiding Question: What are system vulnerabilities and how can systems be hardened?

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).

System Vulnerabilities

Slide 1 - Intro Slide

Slide 2 - Vulnerabilities in Digital Products & Systems

Define Vulnerability: Vulnerabilies exist in the code of operating systems, applications and even the firmware for physical devices like webcams.

Slide 3 - Video Part 1

Darknet Diaries - MS08-067 - this video slideshow (5:42 minutes) was created from a podcast called Darknet Diaries, Episode 57. https://vimeo.com/720905655

The original pocast has been edited down from the original version https://darknetdiaries.com/transcript/57 (59:00 minutes). Part 2 of the clip is in the PPT: Vulnerabilities Exploited +DnD Pt2

About Darknet Diaries: this podcast tells stories about history and events in our digital systems. The official description is "**True stories from the dark side of the Internet"**. This is a podcast about hackers, breaches, shadow government activity, hacktivism, cybercrime, and all the things that dwell on the hidden parts of the network."

Most of the episodes are about an hour so that is too long to use in lessons, but watching this short video is a good opportunity for students to find out about this podcast and possibly start listening on their own.

Slide 4 - Vulnerabilities in the News

1. The Heartbleed Bug - The Heartbleed bug in the Open SSL software allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. https://heartbleed.com/

2. Log4J - is a small open-source Java program used in thousands of products to log or record activity. Also known as the Apache Log4J because it is a project in the Apache Software Foundation. CISA director named Log4J the worst vulnerability she has seen in her career. Resource video for background: https://www.youtube.com/watch?v=XC3Oqn_yADk&ab_channel=CNBCTelevision - only up to 1:20 minutes

Slide 5 – How do you know if a product is secure?

What can consumers do to determine whether a product is safe or how many vulnerabilities have been discovered?

Slide 6 - CVE Database

Several organizations including the US government cooperate to maintain the Common Vulnerabilities & Exposures database. The CVE is a research database to keep track of the known vulnerabilities that exist in operating systems, applications and even the firmware for physical devices like webcams. The slide lists the most common reasoning that a vulnerability exists but browsing through the NVD makes for some interesting reading.

The CVE includes information about how to "fix" the vulnerability, but this usually means you can only MITIGATE the attacks, not to STOP it. That's because it's impossible to stop all possible attacks and breaches. The intent of digital devices is to share, move, modify, and save data so there is no way to make it completely safe unless we unplug the computer and store it in a locked closet.

Slide 7 - Known Vulnerabilities and CVEs

The MITRE organization maintains this research database to keep track of the known vulnerabilities that exist in operating systems, applications, and even the firmware for physical devices like webcams. Browsing through the CVE database makes for some interesting reading!

The example image is for a vulnerability in MAC OS X from May 2022. If exploited, it will either cause the software to crash or it will allow code execution such as malware. The solution is to install the Security Update but until the user clicks "Update", the OS remains vulnerabile.

Slide 8 - Vulnerabilities Exploited

Slide has animations to step through the concepts to understand "exploits".

1. Definition of exploit
2. Clarify how a vulnerability is used by exploit to execute a mal-action.
3. Fixing the code is called a "patch" update.
4. Updating a device with the patch code will make it secure against exploits from that specific vulnerability. Emphasize that updates only secure against specific vulnerabilities, just like vaccines only protect against specific diseases.

Slide 9 - CVE Example for MS08-067

To make sure students connect the story of MS08-67 with the CVE database, this image shows one of the CVEs that was assigned to the MS08-067 vulnerability. Point out that each CVE has details that break down the score to show how the exploit can affect a victim device including specifics about the impact on CIA.

Slide 10 - Video Part 2

This is PART 2 of the Darknet Diaries - MS08-067 slideshow (5:46 minutes), created from a podcast called Darknet Diaries, Episode 57. https://vimeo.com/727626779

Story tells how the MS08-067 became an opening for one of the worst computer worms in history, the Conficker Worm. Finishes by making the point that Updates are one of the most important actions we can take to secure a device.

The original pocast has been edited down from original version https://darknetdiaries.com/transcript/57/ 59:00 minutes.

Slide 11 - Do you install updates?

After the video, ask students, how many of them do software updates as soon as they are available? How many don't update at all if they can avoid it? What are the reasons that students don't click YES or ACCEPT for updates on their devices?

Slide 12 - Activity - Research CVEs for Named Vulnerabilities

Activity: students will understand and be able to use the NIST National Vulnerability Database (NVD) to research vulnerabilites.