Course: Georgia Introduction to Hardware Technology I Module: Cybersecurity

Lesson 8.3: Network Attacks

https://codehs.com/course/16719/lesson/8.3

Description	This lesson is an introduction to network attacks. Students review how data is transmitted over the internet and learn how attacks occur by exploiting vulnerabilities in open ports.
Objective	Students will be able to: • Define vulnerability and exploits • Explain the role of open ports in a network attack • Explain how a network scan can help identify vulnerabilities
Activities	8.3.1 Video: Network Attacks Overview 8.3.2 Check for Understanding: Network Attacks Quiz 8.3.3 Notes: Check for Vulnerabilities 8.3.4 Connection: Bug Bounty Hunting 8.3.5 Free Response: Bug Bounty Hunting 8.3.6 Connection: Common Port Targets 8.3.7 Example: Port Scanner Simulation 8.3.8 Free Response: Open Port Reflection
Prior Knowledge	While these topics are reviewed in the video, students should be familiar with the following before beginning this lesson: • Ports • How data is transmitted over the internet: routers, DNS, packets, metadata
Planning Notes	• This is an introductory lesson that lays the foundation for the different types of malware and cyber attacks. As such, it is important that students fully understand the role open ports play in network security. • Because this is the start of a new unit, consider starting a new word wall to keep track of cyber defense terminology throughout the unit. • There is a handout that accompanies this lesson that introduces students to exploit kits. It can be used as an in-class activity or a homework assignment. Determine how and if this handout will be used.

Standards Addressed

Teaching and Learning Strategies

Lesson Opener:

- Have students brainstorm and write down answers to the discussion questions listed below. Students can work individually or in groups/pairs. Have them share their responses. [5 mins]

Activities:

- Watch the lesson video and complete the corresponding quiz. This quiz is a quick check for understanding [7-10 mins]
- Complete the *Check for Vulnerabilities* activity. [5-7 mins]
    - Review the activity explanation with students to ensure they understand the term “known vulnerability.”
    - Give students time to run the scan on their computer (it should do so automatically).
    - Debrief the discussion questions with students as a class:
        - What do the results reveal about your computer?
        - If the scanner found a known vulnerability, what should your next steps be?
- Complete the *Bug Bounty Hunting* activities (article and reflection). [10-15 mins]
    - This activity uses the Word-Phrase-Sentence Thinking Routine. While this routine helps students make sense of the text, the power of this routine comes more from the discussion around *why* students chose specific words and phrases. Thus, the goal of this activity is less about what bug bounty hunting is and more about students’ reactions to it.
    - Review the directions with students so that students can use the thinking routine while they read.
    - Have students read the article independently.
    - Direct students to the next activity to write their sentence, word, and phrase.
    - Discuss student responses as a class. Focus discussion on *why* certain words or phrases were chosen. What themes emerge as students share? Are there any similarities? Any contrasts?
- Complete the *Common Port Targets* activity. [8-10 mins]
    - Review the questions with students before reading. Note that the guiding questions here are different than the open response questions at the end of the lesson.
    - Read the article as a class or have students read it independently or with a partner. Note that this is a short article and should not take very long to read.
    - Review the answers to the guiding questions as a class to ensure all students have a thorough understanding of the commonly attacked ports before moving on.
- Complete the *Port Scanner Simulation* activity. [3-5 mins]
    - Before beginning the simulation, ensure students understand what Nmap is as well as what command to enter into the prompt (nmap localhost). Note that students must enter the command exactly as is for the simulation to run.

    - Give students time to run the simulation independently.
    - Direct students to move on to the reflection questions when they are done.
- Complete the *Open Port Reflection* activity. [10-12 mins]
    - Use the Think-Pair-Share strategy for this activity:
        - Think: Give students time to answer the questions independently. Note that students may need to move between activities to remember which ports were open in the simulation. As you circulate and review student answers, if you see a variety of different answers for #1-3, bring the class together to ensure students are all on the same page before moving on to #4-6.
        - Pair: Have students share their responses with a partner. Encourage students to revise and add to their answers based on their discussion with their peers.
        - Share: Discuss student responses as a class.

Lesson Closer:

- Have students reflect and discuss their responses to the end of class discussion questions. [5 mins]

Discussion Questions

Beginning of Class:

- What is a network port? Provide one example of a commonly used port.
    - *A network port is a location where information is sent from one computer to another. Common ports: 80 - http; 443 - https; 20/21 - FTP; 22 - SSH; 53 - DNS.*
- How is data sent over the internet?
    - *Data is broken into packets that contain metadata about the location of the destination and the sender. The packets are then sent via routers to their destination.*
- When you think of the word ‘vulnerability,’ what do you think of? What might it mean in the context of network security?
    - *Responses will vary. Sample response: When I think of the term ‘vulnerability,’ I think of a weakness. In terms of network security, this might be a weakness in the network or a place that is easy to access.*

End of Class:

- What is port scanning? What is an open port?
    - *Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities. An open port is a port that is configured to accept packets.*
- What is the purpose of doing a port scan on your device?
    - *A port scan will check for any open ports on your device. This enables you to make sure that there aren’t any unnecessarily open ports.*

	• Prove or disprove: Open ports are a security risk, so you should not have any open ports on your computer. ◦ *While open ports are a security risk, they are necessary in order to send and receive data over the internet. So, there are some ports that will need to remain open even if they leave you vulnerable.*
Resources/Handouts	Exploit Kits (Student) Exploit Kits (Teacher)

Vocabulary

Term	**Definition**

Modification: Advanced	**Modification: Special Education**	**Modification: English Language Learners**
• For students who are interested in diving deeper into Nmap and network scans, encourage them to check out Nmap’s website, download the software, and explore other commands and scanning options.	• Create a handout that includes keywords and their definitions: open port, vulnerability, exploit, scan • Depending on students’ reading level, you may want to differentiate the article in the *But Bounty Hunting* activity.	• Create a handout that includes keywords, their definitions, and an image. Keywords to include: open port, vulnerability, exploit, scan