UNIT 17: Why Is the Internet Vulnerable

Estimated Time in Hours: 7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
3 Ubiquitous Connectivity 1 Ethics	3.2, 3.1	- Research a SOC. Use a vulnerability scanner. - Research the dimensions of Cyber Warfare (Army Cyber Operations).

Guiding Questions:

- What would life be like without the Internet?
- What would it take for the entire Internet to fail?
- How are we targets?
- What can an attacker see?
- How long can an attack last?
- What can an attacker do?
- Who protects the Internet?
- What are the dimensions of cyber warfare?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
3.2 EU: The Internet provides a large attack surface, which offers efficiencies or economies of scale for adversaries.	• Computer, lecture slides, projector, graphic organizers, access to Internet • "What Would Happen If America's Internet Went Down." *YouTube*, uploaded by Tech Insider, 12 June 2018, https://youtu.be/eHfU3W-ClTE • Nakashima, Ellen. "Russian military was	• Have students imagine what would happen if the entire Internet went down. Discuss this. • Show the video linked left. Have students note the 5 core processes. Why would an attacker choose to attack these? • The video mentions Notpetya. Have students read the article linked left. What was the target of the attack? Who was behind it? Why? What was the purpose of the attack? What is a watering hole attack?

	behind 'NotPetya' cyberattack in Ukraine, CIA concludes." The Washington Post, *WashingtonPost.com*, 12 Jan 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html	• Discuss things that could take out the Internet (asteroid collision, global war, solar flare, massive cyber attack). Which are more likely? Why?
3.2.1 LO: Students will analyze how the connected nature of the Internet allows an adversary to reach a large number of devices. 3.2.1b EK: By directing an attack at a collection of devices (or even all devices on a network), an adversary can attack multiple devices simultaneously, in hopes of compromising a few select devices.	• "Cybersecurity and crime | Internet 101 | Computer Science | Khan Academy." *YouTube*, uploaded by Khan Academy, 23 Apr 2019, https://www.youtube.com/watch?v=5k24We8pED8&feature=emb_logo • Crane, Casey. "DDoS Attacks | Re-Hash: The	• Have students investigate the connected nature of the Internet. • Discuss how this connectiveness allows an adversary to reach a large number of devices. • Show video linked left. Discuss ways we are all targets. • Discuss how an adversary can attack multiple devices simultaneously.

3.2.1c EK: An adversary can attack a large number of systems simultaneously, which can impact a large majority of a group of people.	Largest DDoS Attacks in History." Hashed Out, *TheSSLStore.com*, 25 June 2020, https://www.thesslstore.com/blog/largest-ddos-attack-in-history/.	• Discuss how an adversary can attack large systems simultaneously. What are the results of these types of attacks? • Have students read the article on DDoS attacks (linked left). Students should note the how DDoS attacks are measured (packets and bandwidth), types of DDoS attack methods, and pick a DDoS attack listed and summarize it.
3.2.1a EK: Network mapping and recon tools allow an adversary to gain information on remote systems and an opportunity to get control of the system.	• "Greenbone Security Manager Live Demo." *Greenbone.net*, https://livedemo.greenbone.net/login **Username: livedemo / Password: livedemo**	• Ask students what they think an attacker can see during an attack. • Discuss network mapping, network reconnaissance, and vulnerability scanning. Offer example tools of each and explain their purpose. How could these tools aid an attacker? How does a network administrator use this information? Greenbone security, linked left, offers a free live demo of their vulnerability scanner. Allow students to experiment with it or the teacher can use it as a demo and explain how it works.
3.2.1d EK: An adversary can stay undetected for a long period of time suggesting that early detection is key in preventing a large amount of damage. 3.2.2 LO: Students will identify and predict the outcomes of security vulnerabilities at the physical/link layer, the network	• "2019 Cost of a Data Breach Report | Data Breach Calculator." IBM, https://databreachcalculator.mybluemix.net/?_ga=2.268380235.494425760.1589305840-1006873831.1589305840&cm_mc_uid=94402621085815893058404	• Ask students how long they think an attack can last. Have students research the breach report linked left. • Ask students what an attacker can do once he/she gains entry into a system. Discuss vulnerabilities at each level of the OSI model mentioned in the EKs. The resource linked left offers excellent resources for exploring attacks related to these vulnerabilities.

layer, the transport layer, and the application layer. 3.2.2a EK: At the physical/link layer, an adversary who is able to connect to the link can observe, and possibly modify or jam messages on that link. 3.2.2b EK: At the network layer, an adversary may do two things, impersonate an address (spoofing) or disrupt communication (Denial of Service). 3.2.2c EK: At the transport layer, an adversary may disguise their intentions by using port numbers incorrectly or may disrupt the ability of a device to deliver data to the application. 3.2.2d EK: At the application layer, messages sent by the adversary may cause applications to stop working or behave in a way that serves the goals of the adversary, rather than the way they were designed.	&cm_mc_sid_50200000=95192341589305840431&cm_mc_sid_52640000=53766491589305840462 • "Cybersecurity Interactives." E-Mate 2.0, *e-mate-bbc.org*, https://s3.amazonaws.com/e-mate2/Cybersecurity+Interactives/Cybersecurity+Interactives.html	

1.1.2 LO: Students will understand how the role of values and ethics affects political structures, laws, and policy decisions as it relates to cybersecurity. 1.1.2e EK: Professional codes of ethics convey the expected conduct of cybersecurity professionals. 1.1.2b EK: Institution refers to informal norms, shared understandings, and formal doctrines that constrain and prescribe actors' interactions with one another. 1.1.2c EK: Cyberwarfare, cybersecurity and privacy affect and are affected by institutions, political structures and attendant policies. 1.1.2a EK: Political structure refers to institutions, their relations to and interactions with each other, and the laws and norms present in political systems in such a way that they	• "Code of Ethics." EC-Council, *ECCouncil.org*, https://www.eccouncil.org/code-of-ethics/ • "Team Red vs. Team Blue and how to get into Cyber Security – with Brad Wolfenden." *YouTube*, uploaded by Coding Blonde, 10 Nov 2018, https://youtu.be/Mmd_56Y-1Cc • Firch, Jason. Red Team VS Blue Team: What's The Difference?" PurpleSec, *PurpleSec.us*, https://purplesec.us/red-team-vs-blue-team-cyber-security/ • Borkar, Pramod. "Security Operation Center: Ultimate SOC Quick Start Guide." Exabeam, *Exambeam.com*, 24 Jan 2019, https://www.exabeam.com/security-operations-	• Ask students who protects the Internet. How? Discuss that decisions regarding cyber attacks are complex and involve ethics, political structures, laws, and policy. • Focus on the role of ethics in these decisions. Have students read the code of ethics linked left. • Discuss the role of political structures, laws, and policies. • Discuss the role of a red team versus a blue team. Why are both important? Show the video linked left to help students answer this question. Have students read the article linked left. • Using the article linked left, research a Security Operations Center (SOC). Have students map out their own.

constitute the political landscape of the political entity. 1.1.2d EK: Cybersecurity laws reflect values about national security, economic security, welfare of citizens, domestic law and order, and legitimacy of government.	center/security-operations-center-a-quick-start-guide/	
8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order to prepare people for these new types of jobs.	• "The Army Cyber Team." *YouTube*, uploaded by U.S. Army Cyber Command, 18 Oct 2017, https://www.youtube.com/watch?v=IkAwYGXqBz4 • "TRADOC Pamphlet 525-7-8: The United State Army's Cyberspace Operations Concept Capability Plan 2016-2028." Federation of American Scientists, *FAS.org*, https://fas.org/irp/doddir/army/pam525-7-8.pdf	• Remind students that cyber attacks can sometimes result in cyber warfare. Show video linked left. • Using the document linked left, have students research Arm Cyber Operations and the three dimensions of cyber warfare. They should define CyberSA, CyNetOps, CyberWar, and CyberSpt, explaining the role of each and how they interact. • Students should examine a NICE work role. Perhaps communications security manager.