UNIT 18: Cyber Attack Kill Chain

Estimated Time in Hours: 6

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
7 Risk 6 Adversarial Thinking 8 Implications	7.2	- Identify potential adversaries & their motivations. - List & define common system threats. - Examine the cyber kill chain & the layers of control used to defend against it. - Discuss how pen-testers use adversarial thinking & the cyber kill chain to test defenses. - Identify examples of each stage of the cyber kill chain & brainstorm protective measures. - Visit *Have I Been Pwned* to determine if students' email accounts have been compromised in a breach.

Guiding Questions:

- Who is the adversary?
- What does he want? Why?
- How can he adapt?
- What are the stages of the cyber kill chain?
- How do you defend against these?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
7.2.2 LO: Students will be able to describe how the presence of an adversary necessitates that cybersecurity risk is emergent and complex.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Souppaya, Murugiah and Scarfone, Karen, "Guide to Malware Incident	• Show students the following quote by David Berstein: "For every lock, there is someone out there trying to pick it or break it." Do the students agree or disagree with the quote? Why? • Ask students who they think adversaries are (review from previous units). What do they want? How and when will

7.2.2a EK: Adversaries employ strategic reasoning, including where, when, and how they might attack, as well as tactics for evading detection. 7.2.2c EK: Adversaries are self-interested agents whose behavior evolves and adapts in response to their environments and other actors in the system. 8.1.1g EK: The emergence of advanced persistent threats (APTs) have caused changes in the way individuals and companies are secured and who is involved in securing them. 8.1.1g EK: The emergence of advanced persistent threats (APTs) have caused changes in the way individuals and companies are secured and who is involved in securing them.	Prevention and Handling for Desktops and Laptops." SP 800-83 Rev. 1, *NIST.gov,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf • Cichonski, Millar, Grance, and Scarfone. "Computer Security Incident Handling Guide; Recommendations of the National Institute of Standards and Technology." SP 800-61 Rev. 2, *NIST*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf	he try to get what he wants? The questions are difficult to answer, as the abilities and motives vary. This makes cybersecurity complex. • Discuss how adversaries have strategies and adapt the strategies based on the target system and how it is protected. Have students look for and provide examples of this. • Ask students to list some threats to a system (Denial of Service/ Distributed Denial of Service (DDoS),Man in the Middle (MitM), Social Engineering, Malware and Spyware, Password Attacks, Advanced Persistent Threats (APT). Go over the definition of each of these. The publications linked left can assist in teaching these threats and how experts can respond. • Discuss APTs. How does an entity plan for these advanced persistent threats? • Review the incident response life cycle linked left. Why is this life cycle needed? Students did research on this life cycle in Unit 2. Have students pull from this research to review the concepts with the class.
6.2.3 LO: Students will analyze how the cybersecurity attack lifecycle/kill chain is essential to adversarial thinking.	• "What is the cyber kill chain?" *YouTube*, uploaded by IDG TECHtalk, 12 Feb 2019,	• Examine and overview of the cyber kill chain. Remind students that this is just a model and attacks may not follow this exact path. • Show the video linked left to facilitate discussion.

7.2.2b EK: The steps in an attack are footprinting, scanning, enumeration, network mapping, gaining access, privilege escalation, implant, and hiding tracks.	https://www.youtube.com/watch?v=zhCIg4cLemc • "How the Cyber Kill Chain Can Help You Protect Against Attacks." SBS CyberSecurity, *SBSCyber.com*, 23 Aug 2019, https://sbscyber.com/resources/how-the-cyber-kill-chain-can-help-you-protect-against-attacks	• To protect against the cyber kill chain, an entity should have layers of control. These are: detect, deny, disrupt, degrade, deceive, and contain. Have students examine the source linked left to help students see the correlation between these layers and the kill chain.
6.2.3b: Reconnaissance is the first stage in the attack lifecycle, where adversaries gather public information about the target, and scan their networks to identify how best to plan their attack.	• "Rapid7 Under the Hoodie – The Pizza of Doom." *YouTube*, uploaded by Rapid7, 23 July 2019, https://www.youtube.com/watch?time_continue=2&v=PeO3Qs84GqQ&feature=emb_logo • Breaking the Kill Chain: "Breaking The Kill Chain: A Defensive Approach." *YouTube*, uploaded by The CISO Perspective, 5 Feb 2019,	• Next, have the students watch a series of videos that show penetration testers. Explain to students that, while penetration testers use the same cyber kill-chain to test defenses, they do so legally. This video series allows people to see what a potential attacker could do. They will then discuss what the company should do to protect strengthen their security. • Watch video, "The Pizza of Doom," linked left. Ask students to provide examples of reconnaissance the penetration testers used. They then should brainstorm ways to protect against reconnaissance. • Explain the difference between active and passive reconnaissance. Have students watch the Reconnaissance section of the video linked left ("Breaking the Kill Chain: A

	https://www.youtube.com/watch?v=II91fiUax2g • Cichonski, Millar, Grance, and Scarfone. "Computer Security Incident Handling Guide; Recommendations of the National Institute of Standards and Technology." SP 800-61 Rev. 2, *NIST*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf	Defensive Approach"). Students could also pull from the NIST Incident Response Life Cycle publication linked left to brainstorm defensive strategies for each stage.
6.2.3c: Weaponization is the second stage. Based on the information obtained through reconnaissance, the adversary will tailor their toolset to meet the specific requirements of the target network. This often includes coupling remote access with an exploit into a deliverable payload. 6.2.3d: The third phase is delivery, which is the transmission of the weapon to	• Weaponization: "Rapid 7 Under The Hoodie – You Had Me Before 'Hello'." *YouTube*, uploaded by Rapid7, 8 Feb 2017, https://www.youtube.com/watch?v=uYJPH1nct_U&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=5 • Delivery: "Rapid7 Under The Hoodie – Pwned You	• Repeat this process for the rest of the stages of the kill chain. For each stage, explain the concept, have students look for examples in the video and brainstorm protective measures, and then show the correct segment of "Breaking the Kill Chain: A Defensive Approach" to learn best practices regarding the stage. • Note that another step by attackers is often to hide their tracks. Have students investigate ways to do this. Did they see any examples of this in the videos? • Have students visit the Have I Been Pwned website. Here, they can check to see if any of their email accounts have ever been compromised. If any have, ask students if they

the target environment using vectors like email attachments, phishing, websites, and removable media. 6.2.3e: Exploitation is the fourth phase where the code is triggered exploiting vulnerable applications or systems. 6.2.3f: The fifth stage is installation where attackers install a remote access trojan or backdoor on the victim system in order to conduct further operations, such as maintaining access, persistence and escalating privileges. 6.2.3g: Command and control is the sixth phase of the cyber kill chain. With malware installed, attackers now own both sides of the connection: their malicious infrastructure and the infected machine and can now actively control the system. Attackers will establish a command channel in order to communicate and pass data back and forth between the	Twice." *YouTube*, uploaded by Rapid7 8 Feb 2017, https://www.youtube.com/watch?v=QMAJ4bVB3EI&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=4 • Exploitation: "Rapid7 Under The Hoodie – One Man's Junk Is Another Man's Treasure." *YouTube*, uploaded by Rapid7, 8 Feb 2017, https://www.youtube.com/watch?v=QHPSfHsgIEc&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=3 • Installation: "Rapid7 Under The Hoodie – The Cardboard Box." *YouTube*, uploaded by Rapid7, 23 July 2019, https://www.youtube.com/watch?v=gVj-ELJz5u8&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=9	were notified of the breach. Have they changed their password since the breach occurred?

infected devices and their own infrastructure. 6.2.3h: The final stage of the kill chain is actions on the objective. Once adversaries have control, persistence, and ongoing command and communication, they will act upon their motivation in order to achieve their goal(s), e.g., data exfiltration, destruction of critical infrastructure, to deface web property, or to create fear or the means for extortion.	• Command and Control: "Rapid7 Under The Hoodie – Remote Control." *YouTube*, uploaded by Rapid7, 8 Feb 2017, https://www.youtube.com/watch?v=t-yY8sGv4LY&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=2 • Actions on the Objective: "Rapid7 Under The Hoodie – The Bank Job." *YouTube*, uploaded by Rapid7, 8 Feb 2017, https://www.youtube.com/watch?v=_7dj6K4qY7E&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=1 • *Have I Been Pwned?* https://haveibeenpwned.com/	
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.		• For a career, you could discuss a cyber crime investigator.