LESSON: Introduction to SEH

Before you Begin

This is the very first lesson of this course. Instructors should spend little time explaining how to access TDX Arena or how to navigate Canvas. Instructors may want to spin up the first lab of the module to get it ready and stable before doing it live when the lab slide comes up.

For this lesson, instructors are required to ensure the following activities are completed:

- Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
- Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
- Ensure learners are given opportunities for breaks throughout the lesson. The pacing guide below provides recommended breaks. However, there are additional breaks added in the slide deck, please use them only if needed.
- For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, immediately share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regards to the lesson.
- Labs are to be demonstrated live for each module. The demonstration of labs is the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.
- At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with open Q&A.

Summary

In this lesson, learners will explore the concepts of hacking, encompassing both malicious and ethical activities. They will learn about different hacker types and their distinct motives. The roles of red, blue, and purple teams in testing and defending an organization's cybersecurity will be highlighted, as well as the ethical principles that guide cybersecurity professionals. The distinction between information security (InfoSec) and cybersecurity will be clarified, emphasizing their specific focuses. The lesson will introduce the fundamental CIA triad principles and the importance of awareness and education in countering non-technical intrusions, particularly social engineering. Learners will become familiar with various types of malware and their unique malicious activities, including hybrid malware like Emotet.

Additionally, they will understand malware delivery mechanisms and their impact on cybersecurity. Finally, the lesson will cover the cyber attack cycle, providing insights into the systematic sequence followed by adversaries to compromise networks or systems and how to develop cybersecurity strategies to protect digital assets.

Objectives

- Define the concept of hacking.
- Describe the characteristics, motivations, and types of hackers.
- Identify the red, blue, and purple teams and their main responsibilities.
- Recognize ethical hacking principles.
- Explain key concepts within the information security field.
- Describe common social engineering techniques.
- Define malware and its types.
- Identify hybrid malware and provide an example.
- Summarize malware delivery mechanisms.
- Define the cyber attack cycle and describe its stages.
- Explain the case study.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
< 2 min	**Lesson Opener:** Introduction to SEH	● Introduce learners to the importance of SEH in cybersecurity.
< 5 min	**Real World Scenario:** Introduction to SEH	● Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation.
25 min	**Cyber Uncovered:** Hacking Fundamentals	● Begin by discussing the various interpretations of hacking and how it relates to altering software and hardware functionalities. ● Explain the connection between hacking and obtaining unauthorized access, especially in the context of cybersecurity. ● Explore the different motivations behind hacking, including financial gain, espionage, and personal ideologies. ● Describe the categories of hackers, such as ethical hacker, malicious hacker, and ambiguous hacker, highlighting their roles and intentions. ● Introduce the delegation of responsibilities within cybersecurity, focusing on red teams, blue teams, and purple teams. ● Explain the functions and tasks of each team in testing and defending an organization's security posture. ● Present the ethical principles that guide cybersecurity professionals, covering aspects like legality, integrity, professionalism, and responsibilities.

		• Highlight the importance of legal compliance and reliability in ethical hacking practices. • Differentiate between information technology (IT), information security (InfoSec), and cybersecurity, outlining their roles in safeguarding data and systems. • Emphasize the significance of both InfoSec and cybersecurity in protecting an organization's information assets. • Explain the CIA triad principles (Confidentiality, Integrity, and Availability) as the foundation of information security management. • Describe cybersecurity as a dedicated discipline to protect computer systems, networks, and data from various digital threats. • Emphasize the role of cybersecurity in safeguarding individuals and organizations from malicious activities in the digital space. • Provide an overview of social engineering (SE) as a non-technical intrusion technique that relies on human psychology. • Introduce common techniques of social engineering, such as phishing, pretexting, quid pro quo, and tailgating. Emphasize the need for awareness and education to combat these tactics. • Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
5 min Break		
30 min	**Lab:** Cyber Intelligence Gathering	• Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. • Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance.
5 min Break		
25 min	**Cyber Uncovered:** Malware	• Begin by introducing the concept of malware, defining it as "malicious software" designed to harm or operate illicitly within computer systems. • Explain that malware primarily targets computers, networks, or mobile devices, altering their operations and potentially causing various malicious activities. • Discuss common malicious activities associated with malware, including data theft, encryption, deletion, altering or hijacking core computer functions, and monitoring user activities without consent. • Emphasize the need for robust cybersecurity measures to mitigate malware threats and safeguard digital assets. • Introduce the various types of malware, including viruses, worms, Trojan horses, ransomware, spyware, and adware, and describe their characteristics and modes of operation. • Explain the rare but severe cases where malware can cause physical damage to hardware.

		● Highlight the importance of understanding different malware types to better defend against cyberthreats. ● Provide an overview of hybrid malware, discussing its definition and the challenges it poses for cybersecurity defenses due to its adaptability and complexity. ● Use the example of Emotet malware to illustrate how hybrid malware combines attributes from multiple types and evolves over time, highlighting the need for evolving cybersecurity measures. ● Conclude by discussing malware delivery mechanisms, such as phishing emails, drive-by downloads, malvertising, and USB malware, emphasizing the role of both technological vulnerabilities and human behavior in malware distribution. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
30 min	**Lab:** Advanced Malware Investigation	● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. ● Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance.
5 min Pulse Check (wait for ~75% respondent rate then close the poll)		
5 min Break		
25 min	**Cyber Uncovered:** Cyber Attack Cycle	● Provide an overview of FinTrust Corporation, emphasizing its industry, digital infrastructure, and client base. ● Explore the attackers' initial steps, focusing on the reconnaissance phase and the methods used for social engineering. ● Discuss the significance of detailed information gathering and its role in a sophisticated social engineering campaign. ● Examine the tactics employed in delivering the malware-laden payload, emphasizing the use of phishing emails and counterfeit websites. ● Highlight the consequences of employees clicking on the malicious link. ● Dive into the ransomware attack, including the encryption of files and the demand for a cryptocurrency payment. ● Discuss the lateral movement of attackers within the network, emphasizing stealthy tactics and the use of legitimate credentials. ● Explore the attackers' strategy in increasing pressure through threats of data release on dark web forums. ● Discuss the added urgency this threat brought to FinTrust's decision-making process. ● Focus on the importance of continuous monitoring, regular security updates, and maintaining a robust incident response plan. ● Emphasize the role of these measures in early detection, defense against evolving threats, and effective response to data breaches.

		● Discuss FinTrust's response to the cyberattack, including engaging the guidance of a cybersecurity firm and efforts to restore data. ● Explore the long-term consequences on client trust and the company's reputation. ● Conclude by emphasizing the crucial lesson learned: The need for regular employee cybersecurity risk training, specifically on the topics of phishing and social engineering. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
30 min	**Lab:** Introduction to SEH	● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. ● Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance.
10 min	**Lesson Closure**	● For this lesson, spend just a few minutes reminding the learners what the key ”take-aways'' were from the lesson and what they should do to prepare for the next module. The take-aways discussion should include key concepts such as the understanding of hacking vs cybersecurity and knowledge of social engineering as a cyber threat. Students should review this information prior to moving to the next module. ● Recommend that the students read-ahead and come prepared for the next lesson. ● Q&A
	Additional Time Filler (if needed)	● Kahoot ● Discuss interview prep and questioning ● Use breakout rooms for additional lab practice ● Continue Real World Scenario Conversation