LESSON: Brute-Force

Before you Begin

This is the fourth lesson of this course. Instructors should not spend any 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. This is a must do. 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 discuss the intricacies of brute-force attacks, distinguishing between online assaults against active systems and offline attempts against stored data. They will grasp fundamental terminology, understanding the role of passwords in user authentication and the significance of hashes in data security. Exploring common password weaknesses, such as simple composition and reuse, learners will comprehend the vulnerabilities that make systems susceptible to diverse cyberthreats. The lesson will shed light on hashing as a pivotal process for data integrity and authentication, showcasing the distinctions among hash algorithms like MD5, SHA-1, and SHA-256. Learners will explore a spectrum of attack methodologies, including guessing passwords, exploiting default credentials, and employing phishing, thereby gaining insights into tactics employed by attackers. The lesson will elucidate various attack vectors, such as dictionary attacks, pure brute-force, mutated dictionary attacks, and rainbow table attacks, each demonstrating unique strategies for password cracking. Furthermore, learners will understand the cybersecurity challenge posed by offline brute-force attacks, emphasizing the importance of robust defense strategies. Practical tools like John the Ripper, Hashcat, Hydra, and Ncrack will be introduced, providing learners with an understanding of the core tools used for password cracking, while also showcasing features like parallel processing and modular architecture. The lesson will conclude by addressing mitigation strategies against both offline and online brute-force attacks, emphasizing the implementation of robust defense measures, such as strong password policies, hashing, salting, and multi-factor authentication, to safeguard sensitive systems and data.

Objectives

- Define brute-force attacks.
- Explain the concepts of passwords and hashes.
- Explain the hashing process, hash function, and hash types.
- Describe the differences between hashing and encryption.
- Identify attack methodologies and vectors.
- Define offline brute-force attacks.
- Describe the John the Ripper (JTR) tool and explain its sub-tools.
- Explain the hashcat password recovery tool.
- List examples of online hash cracking services.
- Explain the mitigation measures taken to defend against offline brute-force attacks.
- Define online brute-force attacks.
- Explain Hydra and Ncrack and their features.
- Describe the key mitigation strategies for online brute-force attacks.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
< 5 min	**Career Outcomes Content Reminder**	● Remind learners about the Career Outcomes module to ensure that they know that the materials are available and to complete the assigned modules. ● This module will help the learners do the following: ○ Understand why networking is vital for career development and job search success, as well as how LinkedIn can be utilized for networking. ● Learners will receive an email inviting them to create an account for Big Interview. This platform allows them to sharpen their interviewing skills and utilize tools and resources to prepare for the technical interview. Learners who have not received an email should connect with their career coach. They can connect with their SSM if they do not know who their career coach is. ● The Career Outcomes module can be found at the end of Week 2 of Social Engineering and Ethical Hacking. ● Students can reach out to their SSM for questions and help if they need it.

< 2 min	**Lesson Opener:** Brute-Force	● Introduce learners to the importance of brute-force in cybersecurity.
< 5 min	**Real World Scenario:** Brute-Force	● 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:** Brute-Force Attack Fundamentals	● Provide an overview of brute-force attacks, distinguishing between offline and online attacks and emphasizing the role of automated software in generating multiple guesses. ● Highlight the critical factors influencing the effectiveness of brute-force attacks, such as time and the complexity of targeted values. ● Explain the fundamental concepts of passwords, emphasizing their role in user authentication and system access. ● Define hashes and elaborate on their use in representing data, specifically in the context of password security. ● Explore common weaknesses in passwords, including simple composition, reuse, lack of updates, and inadequate length. ● Discuss how each weakness contributes to the vulnerability of passwords and the increased risk of successful brute-force attacks. ● Introduce hashing as a process for converting input data into fixed-size hash values, highlighting its goals of ensuring data integrity, quick data retrieval, and authentication. ● Explain the operation of hash functions, with a focus on notable algorithms like SHA-256 and MD5. ● Clarify the unidirectional nature of hashing compared to reversible encryption processes. ● Describe the authentication scenario where a user's password is hashed and compared to a stored hash value, emphasizing the validation of data integrity without revealing the original password. ● Present the primary distinctions among hash functions, focusing on hash names, descriptions, and lengths for MD5, SHA-1, SHA-256, NTLM, and NTLMv2. ● Discuss the strengths and vulnerabilities associated with each hash type. ● Explore various attack methodologies, including guessing passwords, exploiting default passwords, systematic cracking, and phishing. ● Explain how phishing, although not a brute-force method, complements brute-force attacks by tricking users into revealing credentials. ● Introduce attack vectors like dictionary, pure brute-force, mutated dictionary, and rainbow table attacks. ● Explain the unique strategies employed by each attack vector and their varying degrees of complexity and effectiveness. ● 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.
25 min	**Lab:** Brute-Force Fundamentals	● 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:** Offline Brute-Force Attacks	● Begin the lesson by introducing offline brute-force attacks, explaining that they occur when attackers obtain authentication data (like password hashes) externally, without system interaction. ● Emphasize the challenge these attacks pose to cybersecurity, often stemming from system breaches or leaks. ● Transition to John the Ripper (JTR) as a versatile password cracking tool, detailing its proficiency in cracking various password hash types. ● Illustrate its optimization for speed through parallel password cracking, wordlist and rule-based attacks, and its inclusion in Kali Linux. ● Conduct a demonstration showcasing a basic wordlist password cracking attack using JTR. ● Move on to hashcat, emphasizing its reputation as the world's fastest password recovery tool that supports multiple hashing algorithms. ● Highlight its ability to utilize both CPUs and GPUs for efficient password cracking, along with the extension of attacks through specialized rules. ● Conduct a demonstration of hashcat performing a dictionary attack and recovering passwords from hashes using the rockyou.txt wordlist. ● Introduce online hash cracking services, emphasizing their role in decrypting or cracking hashes through methods like brute-force attacks. ● Showcase CrackStation, Hashes.com, and Fast Hash Cat as examples with extensive computational resources. ● Conclude the lesson by addressing offline brute-force attack mitigation strategies. Stress the importance of strong password policies, hashing and salting passwords, and regularly updating credentials as key defense measures. ● 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.
25 min	**Lab:** Offline Brute Force Attacks on Hashes	● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day.

<table>
<tr><td></td><td></td><td>● Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance.</td></tr>
<tr><td colspan="3"><b>5 min Pulse Check</b> (wait for ~75% respondent rate then close the poll)</td></tr>
<tr><td colspan="3"><b>5 min Break</b></td></tr>
<tr><td>25 min</td><td><b>Cyber Uncovered:</b>
Online Brute-Force Attacks</td><td>● Begin the lesson by introducing online brute-force attacks, emphasizing their direct interaction with targeted systems and the repetitive trials to guess credentials.
● Highlight the contrast with offline attacks, noting the significance of system security measures in detecting and thwarting attempts.
● Transition to Hydra, detailing its role as a highly proficient and parallelized password cracker for conducting brute-force attacks across various protocols.
● Highlight its features, including multi-protocol support, modular architecture, parallelized operations, and its integration with Kali Linux.
● Conduct a demonstration of Hydra performing a dictionary attack on an SSH server, showcasing key components and output details.
● Move on to Ncrack, presenting it as a tool designed for high-speed network authentication cracking with a focus on ensuring robust password policies.
● Outline its features, including modular architecture, versatile targeting, high-speed operation, and pairwise cracking.
● Conduct a demonstration of Ncrack performing a dictionary attack on an SSH server, emphasizing key components and the successful discovery of a password.
● Conclude the lesson by addressing mitigation strategies against online brute-force attacks.
● Highlight the importance of account lockout policies, CAPTCHA mechanisms, and multi-factor authentication (MFA) in deterring unauthorized access attempts and protecting sensitive systems and data.
● 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.</td></tr>
<tr><td>25 min</td><td><b>Lab:</b>
Remote Desktop Brute Force Attack</td><td>● 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.</td></tr>
<tr><td>10 min</td><td><b>Lesson Closure</b></td><td>● 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 understanding Brute-Force attacks and password security as well as tools for</td></tr>
</table>

		mitigation. 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
2 min	**Midpoint Course Survey**	● Allocate 2 minutes to facilitate the completion of the Midpoint Survey. ● Encourage learners to provide honest and constructive feedback about their learning experience.
3 min	**Discussion Board**	● Allocate 3 minutes Review Discussion Board Slides and how it impacts students' final grades.
	Additional Time Filler (if needed)	● Kahoot ● Discuss interview prep and questioning ● Use breakout rooms for additional lab practice ● Continue Real World Scenario Conversation