ADVERSARIAL tHINKING mODULE

**Module Description:** This module provides a basic introduction to adversarial thinking, game theory, and behavioral game theory to help develop cybersecurity students’ abilities to anticipate the strategic actions of cyber adversaries, including where, when, and how they might attack, and their tactics for evading detection. This module’s content is the subject of two peer-reviewed journal articles.

**Prerequisite Knowledge:**  This is a stand-alone, self-contained module that can be incorporated into any cybersecurity course at any university level. There are no knowledge prerequisites for this module.

**Length of Completion**: This module contains three lessons of approximately one hour each.

**Level of Instruction:** This module is appropriate for both technical and non-technical students of all university levels.

**Learning Setting:** This module is intended to be taught in-class by an instructor.

**Instructor Reference Material:** Instructors may find it helpful to review the following primary source material in preparation for teaching this module:

* S. Hamman and K. Hopkinson, “Teaching Adversarial Thinking for Cybersecurity,” *Journal of The Colloquium for Information System Security Education*, vol. 4, no. 1, pp. 93-110, 2016. [Available from CISSE archives: https://cisse.info/resources/archives/category/41-papers]
* S. Hamman, K. Hopkinson, R. Markham, A. Chaplik, and G. Metzler, “Teaching Game Theory to Improve Strategic Reasoning in Cybersecurity Students,” *IEEE Transactions on Education*, vol. 60, no. 3, pp. 205-211, 2017. [Available from IEEE Xplore Digital Library: http://ieeexplore.ieee.org/document/7809088/]

**Activities:** There are two learning activities for each of the three lessons for a total of six learning activities:

1. Data Breach
2. The Cuckoo’s Egg
3. The Battle of Bismarck Sea
4. Solomon’s Wise Ruling
5. The 2/3s Guessing Game
6. DDoS Attack

# learning outcomes

MODULE learning oUTCOMES

* Students will be able to analyze cybersecurity from the strategic perspective of cyber adversaries.

# module Details

**Interconnection:** This module has no interconnections with other modules.

**Instructional Files and Online Resources that are Needed:**

* Lesson 1 – Intro to Adversarial Thinking.pptx
* Lesson 2 – Intro to Game Theory.pptx
* Lesson 3 – Intro to Behavioral Game Theory.pptx
* Data Breach Exercise.docx
* The Cuckoos Egg Exercise.docx
* The Battle if Bismarck Sea Exercise.docx
* Solomons Wise Ruling Exercise.docx
* The Two Thirds Guessing Game Exercise.docx
* DDoS Attack Exercise.docx

**Assessment:** Instructors, please contact the author of this module for the assessment materials – contact info available on CLARK and in the title slide of each lesson.

# lessons

**Overview of Lessons:**

Lesson 1 – Intro to Adversarial Thinking

Lesson 2 – Intro to Game Theory

Lesson 3 – Intro to Behavioral Game Theory

**Lesson 1 Learning Outcomes:**

Upon completion of this lesson:

* Students will be able to illustrate the three components of adversarial thinking for cybersecurity.

**Lesson 1 Details:**

**Warm Up:** Data Breach

**Lesson:** Intro to Adversarial Thinking

**Active Learning Activity:** The Cuckoo’s Egg

**Lesson 2 Learning Outcomes:**

Upon completion of this lesson:

* Students will be able to analyze a strategic scenario from a game theoretical perspective.

**Lesson 2 Details:**

**Warm Up:** The Battle of Bismarck Sea

**Lesson:** Intro to Game Theory

**Active Learning Activity #1:** Solomon’s Wise Ruling

**Active Learning Activity #2:** The Battle of Bismarck Sea – Revisited

**Lesson 3 Learning Outcomes:**

Upon completion of this lesson:

* Students will be able to apply level-*k* reasoning to derive playing strategies in strategic contests.

**Lesson 3 Details:**

**Warm Up:** The 2/3s Guessing Game

**Lesson:** Intro to Behavioral Game Theory

**Active Learning Activity:** DDoS Attack

**Wrap Up:** Data Breach - Posttest