10-2020

Development and Assessment of Courses in Defensive Security and Ethical Hacking

Pann Ajjmaporn

Jeremy Straub

Development and Assessment of Courses in Defensive Security and Ethical Hacking

Pann Ajjimaporn, Jeremy Straub
Department of Computer Science, North Dakota State University

ABSTRACT

In order to combat the malicious actors of the digital age, cybersecurity experts have quickly become essential in almost every company [1]. New employees must be ready to 'hit the ground running' in this dynamic and frequently changing field. To effectively prepare students for careers in cybersecurity, enhancements are needed to traditional class-based lecture techniques. This work presents and evaluates two different methodologies used in cybersecurity education: a gamification approach which used a capture the flag model and competition-based approach.

INTRODUCTION

CAPTURE THE FLAG

Capture the flags (CTF) is a traditional game which involves so-called flags that competitors attempt to access and collect. The online game is named after a children's' game where competitors traverse a field and grab flags from their opponent.

- In the cybersecurity field, CTFs are digital 'wargame' challenges with scoring similar to the traditional capture the flag game [2].
- The flag in the online CTF is be a string of text, and the field is system that students must access or the puzzle that they must complete.
- In order to obtain the flag, competitors must accomplish tasks, such as gaining access to a database, completing a challenge or filtering through log data, etc., to find it.

Figure 1. Example of CTF flag

COMPETITION-BASED METHODOLOGY

Competition-based learning (CBL) is a learning pedagogy that combines problem-based learning paradigms with competition.

- Competition-based learning involves a scoring system (beyond grading) to provide students motivation based on peer competition [3][4].
- It is modeled after workplace competitiveness.

METHODOLOGY

Data related to student perception and learning was gathered via surveys conducted in cybersecurity courses along with a pre-test exam and final exam. Courses had relevant features:

- CTF – In this class, students performed CTF examples for each major cybersecurity topic for potential extra credit in the class.
- Competition-based – In this class, a review quiz for each chapter was performed in a competitive manner using Kahoot. High scoring students received extra credit in the class.

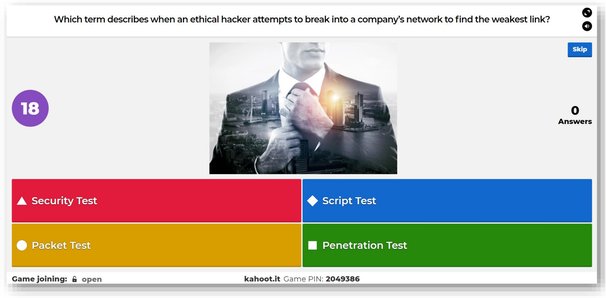


Figure 2. Example of Kahoot quiz

Two types of data collection were used in each class:

- Academic performance – the midterm and the final exam of the class. Comparing pre-test results and student performance on the midterm and final provides information about student learning of course material.
- Student satisfaction – asked students for their opinion regarding the game-based and competition-based elements and their enjoyability and effectiveness in helping students learn and retain class material.

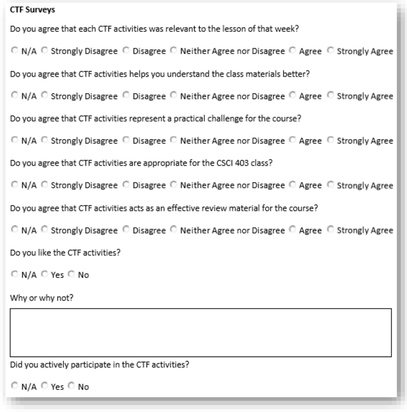
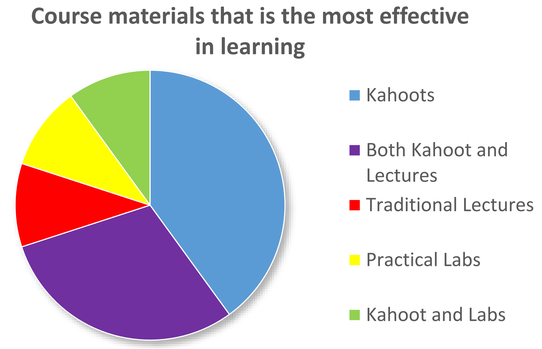


Figure 3. Example of survey questions.

RESULTS

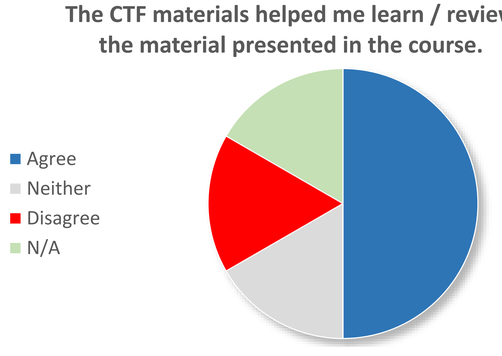
The chart below shows the course materials that the students have identified as being the most effective in facilitating their learning of the class material.

- Overwhelming majority of the class identified the Kahoot competition as the most effective teaching tool.
- There were also students who preferred the traditional lecture slides, in combination with the competitive element, as well.
- This chart shows that not every student preferred a single educational technique. Instead, this indicates that the use of a combination of multiple techniques throughout the course is beneficial.



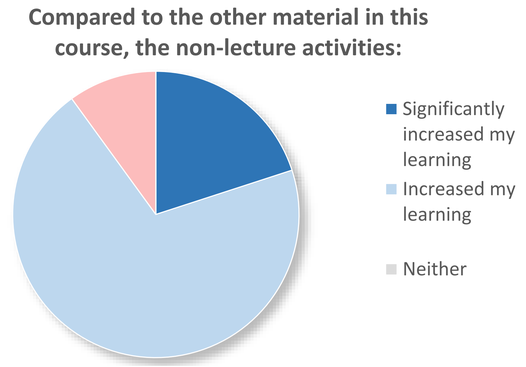
The survey results suggested that the non-traditional approaches used in the class enabled students to learn the cybersecurity materials in a more engaging manner.

- Notably, a small percentage of the students indicated that the extra activities distracted from the traditional learning process.
- Approximately half of the students indicated that the CTF exercises were helpful. Only 17% did not find the CTF helpful.



RESULTS

The feedback for the competition approach also reinforces this idea. This was suggested by most of the "short answer" format questions in the survey as being very positive and, as shown below, increased students learning.



CONCLUSIONS & FUTURE WORK

- This work showed correlation between student participation in non-traditional activities and better-than-average performance.
- A larger sample size is projected to show a clear increase in both the level of engagement of the students and their knowledge of the materials.
- Future work is planned to assess the correlation between specific course material and particular methodologies to identify the most effective way to present each type of cybersecurity course content.

REFERENCES

[1] McDonald, Clare. "*Rise in IT security demand triggers surge in cyber security jobs*", computerweekly.com [2015]

[2] C. Cowan, S. Arnold, S. Beattie, C. Wright, and J. Viega, "Defcon Capture the Flag: Defending vulnerable code from intense attack," in Proceedings - DARPA Information Survivability Conference and Exposition, DISCEX 2003, 2003, vol. 1, pp. 120–129, doi: 10.1109/DISCEX.2003.1194878

[3] Chung, CJ. "CBL: Competition-Based Learning Learning through Competitions-Competition-Based Learning (CBL)", Conference at Lawrence Technological University, April 2008

[4] Duffrin, Willard, M.W. "Utilizing Project-Based Learning and Competition to Develop Student Skills and Interest in Producing Quality Food Items". Vol. 2, 2003—JOURNAL OF FOOD SCIENCE EDUCATION