A Capture The Flag (CTF) Platform and Exercises for an Intro to Computer Security Class

Zack Kaplan
zack.kaplan@wustl.edu
Washington University in St. Louis
St. Louis, Missouri, USA

Ning Zhang
zhang.ning@wustl.edu
Washington University in St. Louis
St. Louis, Missouri, USA

Stephen V. Cole
svcole@wustl.edu
Washington University in St. Louis
St. Louis, Missouri, USA

ABSTRACT

Cybersecurity education is becoming increasingly important as demand for cybersecurity professionals increases. Hands-on skills are a critical component of cybersecurity education, and a variety of exercise types have been developed to teach these skills. In this work, we seek to apply the benefits of gamified learning to an introductory cybersecurity curriculum in the form of a set of Capture the Flag (CTF) challenges offered as hands-on exercises for an intro-level course. We created 20 jeopardy-style challenges of varying difficulty based on prior research on the use of gamification in education, and we configured the open-source CTFd platform to host our challenges. Student responses to post-challenge surveys suggest that the CTF component of the course was effective in improving perceived learning and student engagement.

CCS CONCEPTS

• **Security and privacy**; • **Social and professional topics** → **Computer science education**;

KEYWORDS

CTF, Capture The Flag, cybersecurity, gamification, student engagement, hands-on exercise

ACM Reference Format:
Zack Kaplan, Ning Zhang, and Stephen V. Cole. 2022. A Capture The Flag (CTF) Platform and Exercises for an Intro to Computer Security Class. In *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol 2 (ITiCSE 2022), July 8–13, 2022, Dublin, Ireland.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3502717.3532153

1 INTRODUCTION

To address the increasing demand for cybersecurity professionals with hands-on skills and the projected deficiency in qualified security professionals over the next several years [1], security educators have developed a variety of hands-on exercises to complement traditional learning methods. One of the most widely deployed sets of exercises for college-level cybersecurity classes is the SEED Labs[1], which cover a wide range of security topics from systems security to web security and run on a freely-available customized VM image.

To offer students the benefits of gamification for student engagement and learning outcomes [3][4] in our Intro to Computer Security course, which has used several SEED labs as a subset of our hands-on exercises for multiple semesters, we developed and incorporated Capture The Flag (CTF) exercises augmenting our existing hands-on exercises in the Summer 2021 and Fall 2021 offerings of the course. We used single-player "jeopardy-style" puzzle-solving CTF challenges suitable for incorporation into a typical security course as assignments. The hallmarks of such challenges are that they have a tangible token of successful completion – usually an un-guessable text string a player discovers when she solves the challenge – and that they are deliberately under-specified in their solution path to varying degrees, so that a player must exercise ingenuity or do outside research to solve the challenges.

In this work, we present the CTF platform and exercises developed for the course, and report on the implementation of the exercises as measured by a student survey taken upon the completion of the CTFs. Because all the CTF exercises are designed to reinforce concepts in the SEED labs, we hope many will be of direct interest to the cybersecurity education community.

2 RELATED WORK

Previous work on CTFs in cybersecurity education has shown that they produce positive learning outcomes, improved grades, and increased confidence in cybersecurity skills (see [2, 5] for examples). Our work is novel in (1) designing many new CTF challenges specifically to complement the hands-on exercises in our Intro to Security course, including the SEED labs used in the course, and (2) in configuring the CTFd platform for a smooth, repeatable, extensible hosting of this set of challenges by future instructors at our own or other institutions.

3 PLATFORM AND EXERCISES

3.1 CTF Hosting

To create and host the CTF challenges, we used the popular open-source CTF-hosting framework CTFd[2] to publish challenges and track student progress, with a campus-network-connected Linux server hosting our CTFd instance. Students created accounts using their school email addresses, and interacted with the server via a web browser to complete challenges and earn points. CTFd supports the import/export of challenge configuration files, allowing for easy plug-and-play setup and backup for hosts or instructors. Features such as progressive unlocking of challenges allow instructors to

[0]This work is supported in part by the U.S. National Science Foundation under grants CNS-1916926 and CNS-2038995.
[1]https://seedsecuritylabs.org/

ITiCSE 2022, July 8–13, 2022, Dublin, Ireland

ACM ISBN 978-1-4503-9200-6/22/07.
https://doi.org/10.1145/3502717.3532153

[2]https://ctfd.io/

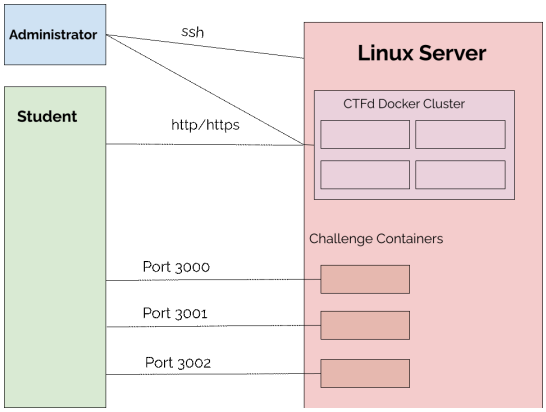

Figure 1: Server architecture and connection types for the course's CTF system. The administrator uses ssh to set up Docker containers (including one for CTFd) on the server, which are then accessible to users. CTFd is configured through a web interface after the containers are launched, and challenge containers have their own separate ports for remote connections.

enforce dependency chains in completing exercises and to pre-publish all exercises for a course at the beginning of a term, and features such as an automatic scoreboard allow students to easily track their own progress throughout the semester.

3.2 CTF Challenges

A series of 20 CTF challenges were created for this work. The challenges fall under the general categories of Encryption, Networking, Linux, Web, Steganography, and Exploitation, and comprise 3 server-style challenges requiring Docker containers, 11 challenges adapted to CTF style from course assignments and labs, 4 custom-built CTF-style challenges, and 2 lightly-modified challenges based on previous CTF competitions. Twelve easier challenges require the straightforward application of course material and SEED lab knowledge and were worth 10 points each, while eight harder challenges require creative application of course material or outside research and were worth 20-50 points each. Challenges include:

- A 10-point challenge requiring students to decrypt an encrypted message using openSSL (a tool used in a corresponding SEED lab), with a riddle giving hints about the Key and IV encryption parameters needed to complete the decryption.
- A 20-point challenge requiring students to use a brute-forcing tool to crack the password of an encrypted zip folder.
- A 20-point challenge requiring students to ssh into a container and find different user credentials for the same container, then log in with those new credentials and search through the many files on the system for the flag using common Linux techniques.
- A 50-point challenge requiring students to execute a buffer overflow exploit on a vulnerable program.

All challenges were designed to be light-hearted, with many jokes and puns (designed with diversity and inclusion in mind) scattered throughout the instructions and hints, in order to promote enjoyment and decrease stress when solving.

Table 1: Post-CTFs survey results: average ratings of the perceived impact of the CTF challenges on the categories shown. Response options ranged from 1 (strong negative impact) to 5 (strong positive impact).

Prompt	Avg. Rating	Std. Dev.
Learning Experience	4.06	0.70
Understanding of Course Material	3.88	0.89
Security Skills Improvement	4.06	0.79
Security Skills Confidence	3.88	0.93
Engagement vs. Other Course Material	4.00	1.00
Course Performance	3.67	0.96
Overall Cybersecurity Understanding	3.94	0.75

4 IMPLEMENTATION

The CTF platform and challenges were presented during two sessions of the class, once as a pilot run during the Summer 2021 session and once during the Fall 2021 session.

For the Fall 2021 offering, participation was required in that the equivalent of completing all 10-point challenges counted as a graded assignment in the course, and earning additional points counted for extra credit. A survey collecting learner feedback on the CTFs was given to students most of the way through the session, and counted as the equivalent of a 10-point challenge toward their grade. The survey asked students to rate the CTFs' impact in several items on a 5-point Likert scale, with 5 representing a strong positive impact and 1 representing a strong negative impact.

5 SURVEY RESULTS

Results from the n=33 survey respondents are summarized in Table 1. The results suggest that students perceived increased engagement and positive learning outcomes across a variety of metrics from working on the CTFs.

6 MATERIALS

All necessary files and instructions for setting up and managing the CTF challenges are stored in a Github repository accessible to course instructors and available to other instructors upon request.

REFERENCES

[1] William Crumpler and James A Lewis. 2019. The cybersecurity workforce gap. Center for Strategic and International Studies (CSIS) Washington, DC, USA.
[2] Juho Holmi. 2020. Advantages and challenges of using capture-the-flag games in cyber security education. Bachelor's Thesis, University of Oulu.
[3] Chanut Poondej and Thanita Lerdpornkulrat. 2016. The development of gamified learning activities to increase student engagement in learning. *Australian Educational Computing* 31, 2 (2016).
[4] Johnmarshall Reeve and Woogul Lee. 2014. Students' classroom engagement produces longitudinal changes in classroom motivation. *Journal of educational psychology* 106, 2 (2014), 527.
[5] Daniel Votipka, Eric Zhang, and Michelle L Mazurek. 2021. HackEd: A Pedagogical Analysis of Online Vulnerability Discovery Exercises. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1268–1285.