ISSN 1870-4069

Using CTF Tournament for Reinforcing Learned Skills in Cybersecurity Course

Hugo Gonzalez, Rafael Llamas, Omar Montaño

Universidad Politécnica de San Luis Potosí,
Academia de Tecnologías de la Información y Telemática,
San Luis Potosí, SLP, Mexico
hugo.gonzalez,rafael.llamas,omar.montano @upslp.edu.mx

Abstract. In this paper, we present an experience on using CTF tournament as a gamification process to reinforce learned knowledge and skills on cybersecurity course. It is important to highlight that part of those skills learned were defined by the students during the course. This strategy was used to improve the students' engagement, at the same time to fulfill as much as possible the expectations for the class. The results of the tournament and final surveys at class showed that it was a good experience for the majority of the participants. The results showed that it helped to reinforce the learned skills, and applying them to specific challenges. The students felt motivated and productive when they were able to solve a challenge.

Keywords: CTF tournament, learning skills, cybersecurity.

1 Introduction

Learning through practice is a common philosophy for some teachers, including the authors of this work. Some courses in different fields in computer science include well-established practices and activities. In those activities, the student is guided to achieve some very specific goal related to the course. Sometimes there is a gamification component if the instructor set a realistic game to test the students in a real-world case scenario in a controlled environment. However, this is not always the case.

In cybersecurity field, there had been several studies talking about setting up capture the flag (CTF) games as part of the course [4], or use it to teach basic cybersecurity skills and generate engagement on the topic for high school students [14]. Other scholars discussed the participation in national wide CTF tournaments to improve skills of students [8]. However, in this work we propose a slightly different approach: Using an extra class CTF tournament to reinforce knowledge and skills learned during a cybersecurity course.

There are mainly two types of CTF, one focus on attacks and defense, and another type that employs a jeopardy style. Jeopardy style CTF are developed as a set of challenges in different domains as such as network analysis, web hacking, forensics analysis, reverse engineering, cryptography. For each domain, a series of

challenges are designed with increasing complexity than the previous. The points awarded for a solved challenge reflects the complexity of that challenge. Easy challenges will motivate participants on taken next levels of the competition.

The remainder of this paper is organized as follows: In Section 2 we describe our experience in running a CTF tournament. In Section 3 we present the results, Section 4 briefly present related work. Finally Section 5 concludes this work.

2 Our Experience

At the Polytechnic University of San Luis Potosi, we offer one shared course about Information Security for two of our programs: Information Technologies and Telematics. Previous experiences showed us that the technical skills, knowledge, and interest about cybersecurity could be very different among the students of a class, from the one not really interested in the topic to the one that expends nights learning and practicing cybersecurity topics by herself. Those differences create an environment where engagement can be low and expectations can be very high from different students.

To address that matter, we decide to improve the engagement of the students and fulfill the expectations of the class as much as possible. As the use of gamification had been proposed before [9], we focus our efforts in a CTF tournament along the flexibility that we have to adapt locally the syllabus of the course. Previous effort on a CTF tournament was poorly received by the students, with only one team registered. This time we took a different approach, the students were involved in define part of the current course syllabus with the objective to increase the engagement in the class and to improve the response on the tournament.

Adaptation process of the syllabus Our course content is organized in three parts: The **first part** is an introduction to cybersecurity, it includes a cybersecurity path as a professional. The **second part** is about information security management systems (ISMS) and their impact at organizations. The **third part** is about advanced topics such as Ethical hacking, and Forensics Analysis.

During spring 2018 term we implemented "research, propose and vote" methodology, a democratic activity to add other topics of interest to the content of the course. At the end of the second part of the course, we asked the students to read the news and search for interesting topics in the cybersecurity field. Then we ask the students to propose one or two topics to be included in the list of options. Finally, we promoted a voting exercise, where each student cast three votes for the topics listed that should be covered in the course. The objective was to increase the engagement of the students and fulfill their expectations on the course. At the same time, we want to make them feel that they were helping to shape the course content on their own interest. Some advanced topics such as low-level attacks were proposed during this activity, surprising the instructors. We combined some of the topics to cover most of the expectations for students with advanced skills.

Part of the activity is shown in Figure 1, after the students proposed the topics and voted for their choices. From the list of options, five topics with the major votes were selected to prepare five laboratory practices to perform during the Third part of the curse. It is important to highlight that the instructors tried to minimize their influence on the selected topics, only discarding non-related topics. However, it was expected to have at least one laboratory practice on forensics and other related to ethical hacking.

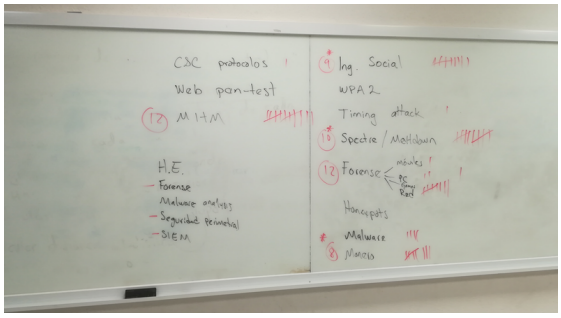

Fig. 1. Cybersecurity topics proposed by the class and voting results.

The selected five topics and their objectives are:

1. Man in the Middle Attack. Perform an attack on a mobile device to capture credentials and other interesting info.
2. Network forensic analysis. Given a file with a network traffic capture, use tools to answer 5 questions about the activities captured.
3. Social engineering. Watch two videos about social engineering attacks and develop a script to apply social engineering to the caller next time they get a phone call that they are not expecting.
4. Spectre and Meltdown attacks. Read an article about these new attacks and execute a proof of concept code in different computers to observe the results.
5. Analysis of a monero miner. Perform a light and superficial analysis of a malware known to mine Monero cryptocurrency to identify the wallet used by the attacker.

CTF design The objective is to create a CTF tournament that includes most of the topics from the adapted syllabus as challenges, including other topics of interest. It is important to note that this tournament should be open to all students at the University during the Information Technology Engineering academic event. But with the original purpose in mind, the students from Information Security courses should receive a special invitation to participate in the tournament to reinforce their knowledge and learned skills. The CTF tournament software selected is Mellivora [15], which is a Jeopardy-style management system

and scoreboard. The challenges should be designed and prepared independently from the platform. Eight categories were created with two to four challenges each. Three of these categories are directly related to the practices in the Third part of the course, four are related to other general topics such as programming. The category *Firmware* is beyond the material covered in the course, this is a challenge to discover and learn new tools and methods under the pressure of the tournament with limited time. Categories, challenges, points available and percentage of teams that solved them are shown in Table 1.

The name of each category intents to be self-descriptive, the categories and challenges that were not solved during the tournament are commented below. Note that the full description of the challenges and the challenges themselves are available upon request to the authors. Help and guidance to create or organize CTF are also offered by the authors.

Firmware category included two challenges, each of them is a firmware for a different device with a modification inside that includes a flag. One modification is a web shell in the admin page. The other firmware contains an extra file with the flag in it. **Programming** category is related to terminal interaction, a student needs to interact with a program 100 times before it returns the flag. These challenges were related to **network programming** category, but instead of sockets, one needs pipes or other methods to interact with other terminal programs in Linux. Both of the challenges include a timer to avoid students to solve them manually. Interacting with the terminal is not a common topic, and the students focus on the rest of the challenges.

The categories that were completely solved are: **Forensics** and **Network Forensics**. The students showed great performance in this categories as they had some similar exercises at class. Also, extra credits for the Information Security course were offered to the team that solved these challenges.

CTF tournament As mention before, the tournament was held in conjunction with an academic event with talks and tutorials some weeks before the end of the term. The tournament lasted two days, access to the challenges were only possible in a classroom assigned to this activity. Five teams of four students and one team of three students were registered. Three teams included at least one female student. Only one registered team was not taking the Information Security course at that term but already took the course before.

Four pictures from the scoreboard and students are showed int Figures 2,3,4 and 5. *ch0co* team won the tournament with 1050 points. **Firmware** category that includes modified firmware for IoT devices were not solved by any team, as this challenge was out of the scope from the course. However, students made comments about these challenges: " [the challenges] were fun to try". The **Web** category was also out of the scope from the course, but most of the students had previous experience with web systems and completed this set of challenges that they considered "not that complicated".

The excitement showed by team members when they capture a flag was contagious and invigorating. Flag after flag they were demonstrating their acquired knowledge during the Information Security course, reinforcing their skills

Table 1. CTF categories and challenges.

Category	Challenges	Points	solved rate
Firmware	Openwrt compromised image	90	0%
	Dlink firmware compromised	110	0%
Forensics	Evidence file	40	100%
	A different flag in the system	90	100%
MITM	Go http test	80	0%
	APK hidden flag	100	50%
Network Forensics	Insecure communications	30	100%
	Binary on the network	60	100%
	Weird binary on the network	100	50%
Network programming	Operations over the network	60	17%
	Something like echo	70	17%
	Strings manipulation over the network	90	17%
Programming	Console interactions	50	0%
	Random strings	70	0%
	Calculate the result	90	0%
Reversing	Go go parameters	70	33%
	Obfuscated Javascript	70	50%
	DotNet mistake	100	50%
Web	Hidden flag	20	83%
	Find the flaw	60	66%
	Enjoy the milk	80	83%
	Official client	80	50%

by playing the game. Some students stated that they learned new skills and abilities during the tournament.

3 Results

The results obtained from this experience are two-fold. First, the students felt engaged and motivated on the class after the "research, propose and vote" process. Second, the students that participated in the CTF tournament described a great experience from the game, solving challenges and applying previous and new skills. The impact of the first result was measured using a survey. In that survey, we asked questions related to the feelings and perception from the students about the process to add topics to the syllabus' course. Also with the engagement and feelings toward the course, expectations and the topics covered. The results of the survey are summarized as follows:

1. The students felt that they are contributing to decide their path on the learning process. They would like to have more courses with a flexible curriculum where they can propose new and interesting topics.
2. The students reported that they were more engaged and motivated in the class, most of them felt that their expectations about the course contents were fulfilled in the class.

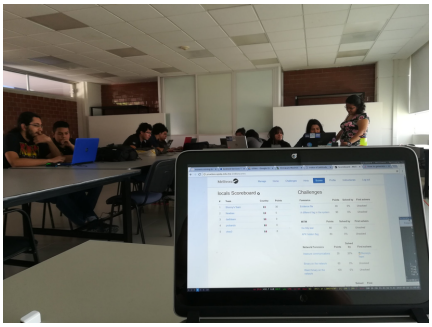

Fig. 2. First flag captured.

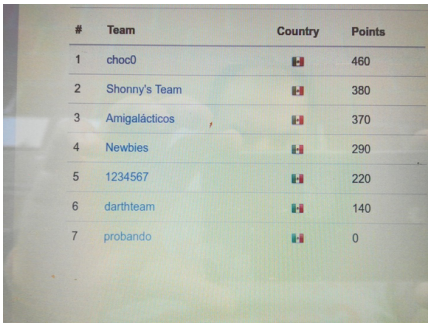

Fig. 3. Scores at the end of the first day.

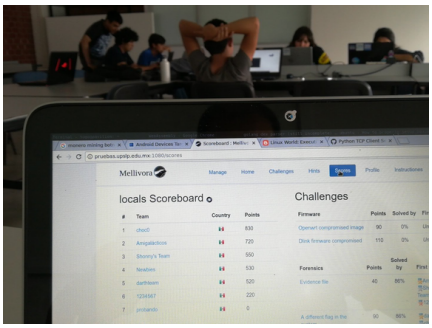

Fig. 4. Working hard on the second day.

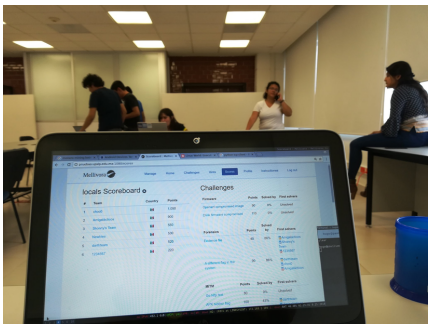

Fig. 5. Final scores.

3. Majority of the students felt well working on the practices. Only two students expressed they were not comfortable with the practices because they found them very technical, and found themselves lacking skills to complete the exercises.

In a blank space to express themselves, some students commented in the survey that they really enjoyed the CTF tournament and that it should be offered every year.

In relation to the CTF tournament, we collected the following information:

More than 60% of students taking Information Security courses registered for the CTF tournament. They expend over 20 hours in the classroom working on the challenges. We consider that the engagement of the students in cybersecurity activities is growing in our university, we believe that this is in part because the gamification strategy introduced in the course. A few students expressed the intention to follow cybersecurity careers.

The overall results of the tournament showed that all teams solved basic challenges on **Forensics**, reinforcing the skills learned at class. Furthermore,

some challenges out of the topics from the class in **Web** category were also solved, showing that students can apply their skills to different problems.

The winning team of the tournament solved 65.2% of all the challenges during the two days competition. Their comments were related to open the game to play outside of the University facilities because they could not play at night from home. That team was suggested to play in the HackDef 2018 CTF pre-qualification tournament [10] that will be held in August.

As feature work, we already started to plan the next CTF game with the format proposed by Chothia et al. [4, 5]. The game will be deployed as an independent virtual machine and will employ an intelligent agent to interact with the students while they are solving the challenges to obtain the flags. The challenges will be related to the topics selected by the class in the term in the course.

4 Related Work

Deterding et al. [7] define "gamification" as the use of game design elements in non-game contexts. Among other tasks gamification is used to engage users and help with the learning process [11]. Recently Li and Kulkarni [13] concluded that gamification is a very effective way of learning.

Gondree et al. [8] discuss the cybersecurity competitions and games and how it is necessary to adopt a common vocabulary to express the game's goals and characteristics. They also discuss about competitions like iCTF, DC3 Forensic Challenge, CyberPatriot, CCDC, PlaidCTF, CSAW CTF where training and education are their main role. At least three frameworks to deploy Capture the Flag contests are freely available as open source software [16, 12, 1].

Chothia et al. had been working in innovation and development of improved course materials. In 2015 the authors presented an offline CTF system which includes 5 learning activities [4]. The students can download the system and play in a controlled environment. In 2016 the authors developed a new course on penetration testing using IoT devices, this course was thought at Birmingham University with great engagement and response from students [6]. In 2017 the authors included a storytelling, intelligent component on a virtual machine to teach a course on information security in 11 weeks [3]; students chose their own adventure in the game. In 2018 the authors focused on spear-phishing, challenging the students to produce realistic spear-phishing attempt where a rules engine will decide if it was successful [5].

Chain et al. offered an innovative platform to capture the flag based on cloud offense and defense. After design and implement their platform, they use a survey to evaluate the pertinence of the exercises, time and difficulties of the tasks. [2].

5 Conclusions

Designing and developing the challenges was a fun exercise for the instructors, and playing them was a great activity for the students to reinforce their

skills. The results from the tournament showed that students were learning new skills that they can apply in real-world scenarios. Gamification in the classroom through CTF tournaments should be implemented and practiced in cybersecurity-related courses. As part of the course or as an extra activity. It is important to mention that all the participant students comment that it was fun, challenging and that they learned and enjoyed the extra class activity.

References

1. Boesen, S., Weiss, R., Sullivan, J., Locasto, M.E., Mache, J., Nilsen, E.: Edurange: Meeting the pedagogical challenges of student participation in cybertraining environments. In: Proceedings of the 7th USENIX Conference on Cyber Security Experimentation and Test. pp. 9–9. CSET'14, USENIX Association, Berkeley, CA, USA (2014), http://dl.acm.org/citation.cfm?id=2671214.2671223
2. Chain, K., Kuo, C., Liu, I., Li, J., Yang, C.: Design and implement of capture the flag based on cloud offense and defense platform. In: 2018 IEEE International Conference on Applied System Invention (ICASI). pp. 686–689 (April 2018)
3. Chothia, T., Holdcroft, S., Radu, A.I., Thomas, R.J.: Jail, hero or drug lord? turning a cyber security course into an 11 week choose your own adventure story. In: 2017 USENIX Workshop on Advances in Security Education (ASE17). USENIX Association (2017)
4. Chothia, T., Novakovic, C.: An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15) (2015)
5. Chothia, T., Paiu, S.I., Oultram, M.: Phishing attacks: Learning by doing. In: 2018 USENIX Workshop on Advances in Security Education (ASE 18). USENIX Association (2018)
6. Chothia, T., Ruiter, J.d.: Learning from others' mistakes: Penetrating testing iot devices in the classroom (2016)
7. Deterding, S., Dixon, D., Khaled, R., Nacke, L.: From game design elements to gamefulness: Defining "gamification". In: Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments. pp. 9–15. MindTrek '11, ACM, New York, NY, USA (2011), http://doi.acm.org/10.1145/2181037.2181040
8. Gondree, M., Peterson, Z.N., Pusey, P.: Talking about talking about cybersecurity games. ;login: USENIX magazine 41(1), 36 – 40 (2016)
9. Gonzalez, H., Llamas, R., Ordaz, F.: Cybersecurity teaching through gamification: Aligning training resources to our syllabus. Research in Computing Science 146, 35–43 (2017)
10. Hacker Defender Academy: Hackdef ctf 2018. http://www.hackdef.net, \url{http://www.hackdef.net}
11. Hamari, J., Shernoff, D.J., Rowe, E., Coller, B., Asbell-Clarke, J., Edwards, T.: Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. Computers in Human Behavior 54, 170 – 179 (2016), http://www.sciencedirect.com/science/article/pii/S074756321530056X
12. Joe Moloch: root-the-box framework. https://github.com/moloch--/RootTheBox/, \url{https://github.com/moloch--/RootTheBox/}

13. Li, C., Kulkarni, R.: Cybersecurity education through gamification. American Society for Engineering Education 123th Annual conference and exposition (2016)
14. McDaniel, L., Talvi, E., Hay, B.: Capture the flag as cyber security introduction. In: System Sciences (HICSS), 2016 49th Hawaii International Conference on. pp. 5479–5486. IEEE (2016)
15. Nakiami: Mellivora is a ctf engine written in php. `https://github.com/Nakiami/mellivora`, `\url{https://github.com/Nakiami/mellivora}`
16. The Computer Security Group at UC Santa Barbara: ictf framework. `https://github.com/ucsb-seclab/ictf-framework`, `\url{https://github.com/ucsb-seclab/ictf-framework}`