

Capture the Flag competitions for Higher Education

Giovanni Lagorio¹, Marina Ribaudò¹ and Alessandro Armando¹

¹ University of Genoa, Genoa, Italy

Abstract

To cope with the shortage of cybersecurity professionals, companies, government organizations, military institutions and, finally, academia have launched their cybersecurity training programs to teach prospective cyber-defenders how attackers think and work. In this paper, we present our experience, as educators, in introducing Capture the Flag competitions and ethical hacking among university students; initially only in an informal context, and then as part of a Computer Security class. Thanks to a Boeing company grant, we had the opportunity to organize training paths and final competitions for our students for three consecutive years and report some results in this paper, sharing some pros and cons we experienced. We hope the lessons learned might be helpful for other instructors willing to follow a similar path.

Keywords

Capture the Flag, Cybersecurity, Higher Education

1. Introduction

Information and Communication technologies permeate every aspect of our life. This brings us a cornucopia of advantages but also a number of security implications. The myriad of hardware and software components that surround us (and which we often rely upon) contain vulnerabilities which can be leveraged for malicious purposes. To defend our assets, e.g., IT systems, critical infrastructures, and our privacy we need more than ever cybersecurity professionals capable to identify vulnerabilities and/or counter attacks leveraging the security weaknesses in such systems. Training a competent workforce is not easy. Acquiring the necessary expertise is anything but simple: theoretical knowledge in many different subjects such as operating systems, low- and high-level programming, network protocols, web architecture, cryptography, etc., must be complemented by practical skills, which can be acquired only with hours and hours of practical (i.e., hands-on) activities.

To cope with the shortage of cybersecurity professionals in the last decades, companies, government organizations, military institutions and (more recently) the academia (see Section 2) have launched their cybersecurity training programs to teach prospective cyber-defenders how attackers think and work.

This paper presents our experience as educators at the University of Genoa by introducing an educational project, offered to Computer Engineering and Computer Science students, that


ITASEC'21, Italian Conference on Cybersecurity, April 7–9, 2021

✉ giovanni.lagorio@unige.it (G. Lagorio); marina.ribaudò@unige.it (M. Ribaudò); alessandro.armando@unige.it (A. Armando)

ORCID 0000-0002-6632-1523 (G. Lagorio); 0000-0003-0697-2225 (M. Ribaudò); 0000-0002-5246-2157 (A. Armando)



© 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

completed its third year at the end of 2019. Thanks to the continued support by the Boeing company over three academic years, we had the opportunity to create an innovative training program that: 1. provided students hands-on training in a number of key cybersecurity topics (namely applied cryptography, network security, web security, and binary analysis) previously not included in our students' curricula; 2. offered students the opportunity to assess and improve their skills through the participation in a Capture the Flag (CTF) competition tailored to their level of expertise; 3. provided the teaching staff the means to complement the traditional assessment techniques (usually limited to assess the knowledge and the competence about the subject) with an evaluation of the practical skills of the students. Another goal of the project was to bring students closer to information security issues, which are nowadays recognized of paramount importance for all companies, even for those whose core business is an entirely different domain.

We organized the hands-on training as a series of *informal meetings*, proposed as sessions offered to students on a voluntarily basis. During these sessions students were gradually introduced to the world of CTF competitions which have become rather popular in the last decade, not only among IT experts and cybersecurity professionals but also among motivated young students. We advertised these activities as *ethical hacking* meetings, to motivate students to learn those skills hackers have, e.g., understanding how systems operate and communicate over a network, how they are designed, how they are protected, whether they are vulnerable, and so on, but without forgetting law and ethics.

From the initial idea of informal meetings to bring interested students closer to cybersecurity topics and competitions, things evolved during the three years of the project. The same hands-on activities, initially attended only on a voluntary basis, were later included as mandatory activities of the Computer Security course offered to all students enrolled in the MSc in Computer Engineering. This double nature of the learning activities (both voluntary or mandatory, depending on the course attended by the student) had some pros and cons. Our research goal is to understand whether CTF competitions can be considered an effective way to teach and promote cybersecurity among students. To this end, we will address the following research questions. The first two questions have been addressed, with preliminary results, in [1], while the third one is new.

RQ1 “*How much does hands-on training improves the students' Cybersecurity skills?*”

RQ2 “*Does hands-on training increase the students' interest in Cybersecurity?*”

RQ3 “*Are CTF-like activities appropriate and effective for official evaluation?*”

Solving a challenge in a “real” CTF not only requires the knowledge of the underlying theory and excellent technical skills but also some form of *lateral thinking*, which is very difficult to teach. Could the evaluation of this type of soft skills be perceived negatively by those students who prefer a more notional form of examination? Might the peculiarity of these exercises be ineffective, or even scaring, for beginners?

These are the points we will discuss in this paper, organized as follows. In Section 2, we present some other experiences we are aware of, and then, in Section 3, we describe the Boeing-UniGe Scholarship Project. Some results are presented in Section 4, where we will answer the

research questions motivating this work and summarize the lessons learned. Finally, Section 5 concludes this work.

2. Related work

Before presenting other experiences published in the literature, let us briefly introduce CTF contests. A good starting point to understand this ecosystem and its community is the website CTFtime¹ that continually updates a list of the past, current, and future events.

Competitions can be of different types, can be organized online or on-site, for a public of expert or novice participants. We concentrate here on Jeopardy CTFs, mostly online, continually organized by cybersecurity experts and practitioners, companies like Google and Facebook, and research groups of academia.

Participants are usually organized in teams that compete for a prize or glory: they enroll, play their game, get the corresponding score, and check their worldwide ranking position.

The events have a fixed duration, which is usually from one to a few consecutive days. When the game starts, players encounter a set of problems - the *challenges* - representing complex tasks in different categories, which cover different cybersecurity topics. By deeply analyzing the problems, players learn the right direction regarding techniques and methodologies to solve each of them. Solving a challenge requires to exploit the vulnerabilities (inserted by the organizers) to exfiltrate the *hidden flags*, i.e., secret strings in a given format. Competitions in this format allow participants, and hence students, to think *adversarially*, i.e., to think as an attacker would, and this form of gamification motivates them to learn by doing. Early experiences introducing these competitions can be found in [2] and [3].

The recent work [4] presents an interesting analysis on the topics covered in CTF challenges. The authors have collected and analysed solutions (called *writeups*) of Jeopardy and Attack/Defense competitions advertised on CTFtime since 2012. By computing keywords frequencies in a corpus of more than 8,500 text documents the authors found that the most popular topics represented in CTF challenges are data security (comprising cryptography), network security, and system security. Other topics, such as privacy or cyber law, which are important in study programs, are not usually covered by CTF challenges. As stated by the authors, the creators of CTF primarily focus on technical knowledge and they suggest their work might inspire educators to design new types of challenges to cover also these missing, but important, topics.

2.1. CTFs for higher education

Gamification techniques can be adopted in higher education for several purposes such as increasing motivation, improving learning outcomes and problem-solving skills, favoring team work. This is well established in the context of computer science education as discussed in a recent study [5] which compares the performances of groups of students exposed to gamification techniques against control groups, e.g., their peers involved in more traditional activities.

¹<https://ctftime.org>

Various experiences of gamification in the form of CTF-like competitions have been published in the context of cybersecurity education. The authors of [6] present an extensive survey in which they examined 71 papers on cybersecurity education published at the ACM SIGCSE and ACM ITiCSE conferences. They identify the most common topics covered in the papers, the most prominent target group for teaching interventions, the most common teaching and evaluation methods employed to check students' performance, the sample sizes, and the availability of public datasets. Its extensive bibliography is a good starting point to read about cybersecurity education experiences.

The same research group presents in [7] the experience of introducing CTF challenges as *homework assignments* in an introductory computer security course. These assignments contributed to the final grade of the exam and the authors provide some recommendation for educators willing to follow a similar experience in their educational activities. For example, they suggest to set in advance the rules for students' collaboration to avoid plagiarism, to inform students on the actions that will be taken to check suspicious flags submissions, and to focus on logging features of the CTF platform to get detailed information of the game progress.

Also [8] presents a *competitive teaching* experience to motivate students in their learning tasks. The paper reports about ten years of the experience at Vienna University of Technology where students are encouraged to solve challenges offered through the course platform. The immediated feedback obtained thanks to a grading bot allows them to follow their performance in the course scoreboard. In addition, students get new "titles" ranging from Nobody to Guru and Master Guru when solving more and more challenges.

As another example, the paper [9] presents the use of the Facebook CTF platform to introduce gamification exercises in a computer security course. In this new setting, the authors organised the *lab activities* as short CTF competitions (between 60 to 90 minutes) followed by discussions, after each event. The results of the competitions were used to grade students and the authors report an increase in the lab grade after the introduction of this form of gamification. Questionnaires were used to assess students satisfaction and, in general, students enjoyed this new hands-on practice. Things could be improved, for example, by introducing the evaluation of partial solutions, which are generally not considered in CTF platforms. The exercises should guide students in learning new knowledge while most often CTF events measure skills. This is a challenge for instructors, specially when they start with this novel educational approach.

Our experience shares many aspects with those just introduced, the main difference is that we organized real CTF competitions, with prizes offered by a big company, and used the results to mark hands-on activities for a group of participants.

3. Teaching Ethical Hacking

In October 2017 we announced the first seminar on ethical hacking targeting students in Computer Engineering and Computer Science. The number of attendees was noticeable, confirming our expectation that there was considerable interest in the topic among the students. We then defined a calendar of meetings with seminars on different topics useful to solve CTF challenges. We scheduled the activities on Friday afternoon to maximize participation, in the only slot not used by other official classes, and the "Friday hacking events" started.

Despite the unfavorable hours in the week, the participation was encouraging, with around 50 participants during the first meetings, a number that decreased over time, as expected, when the complexity of the covered topics increased. At the end of the training, we organized the first on-site Boeing-UniGe CTF competition with two prizes for the best-performing students. 32 students attended this event; even though numbers may not seem striking, a small seed was planted, introducing awareness about hands-on cybersecurity training among the students.

3.1. Autumn 2018 and 2019, second and third editions

At the beginning of the a.y. 2018/19 and 2019/20, we advertised the “Friday hacking events” again. We invited voluntary students, but the novelty was that the meetings became *mandatory* for students of the MSc in Computer Engineering attending the Computer Security course.

Hands-on sessions. In both editions, meetings of 2 hours and a half started in October, lasted for ten weeks, and culminated in the final on-site CTF. Participation was very similar in the two editions. We started with around 100 participants and their number decreased to about 75 towards the end, with a drop-off of the beginners who had just begun to enter the field on a voluntary base.

A typical meeting consisted of the presentation of some introductory material so that students could understand the topic, the context, and which are the main techniques and tools useful to detect and exploit possible vulnerabilities in the given context. Afterward, exercises were proposed and solved, some during the meeting, the remaining at home. The topics covered during the seminars are mainstream in ethical hacking, e.g., basics on Linux, programming, network protocols, Web security (client and server), basics on applied cryptography, and on binary reverse engineering.

The meetings were streamed and recorded using YouTube and afterward made available to the students who were unable to attend. Besides this, we set up a Telegram channel for announcements and to share slides and other material. The channel was also used for supporting students beyond classes. To avoid solution spoilers we asked them to “hide” technical questions and solutions, and suggested to use the ROT13 substitution cipher², so that students unwilling to receive any suggestion simply did not convert back the ROT13 channel’s messages.

The platform chosen for the training and for hosting the Boeing-UniGe CTF is *CTFd*³, an open-source software designed to support CTF organizers. CTFd handles the publication of exercises, registration of participants, flag submissions, and automatic scoring. The training platform was left accessible after the end of the hands-on training sessions so to let students to solve and submit their flags even after the completion of the project.

On-site CTF. On December 2018 and December 2019, we organized a 4 hour long, on-site CTF with four prizes to reward the students who performed best.

To meet the *dual role* of the CTF, i.e., a competition among students for a grant and the hands-on part for the Computer Security class, challenges were of two different types. Some, labeled with “*”, were specific for the exam: designed to be less “challenging”, they could be easily solved by merely studying the course material, without any need for lateral thinking.

²<https://en.wikipedia.org/wiki/ROT13>

³<https://ctfd.io/>

4. Results

To answer the three research questions introduced in Section 1, we use different data collected during the last two editions⁴, namely (i) the answers to the anonymous surveys administered at the end of the training, (ii) the two Boeing-UniGe CTFs results and (iii) the marks of the Computer Security (written) exam.

At the end of the training, we counted, on average, around 75 active students in both editions, in a mix of mandatory and voluntary participants. A short survey (see Appendix A.1) was announced via Telegram along with a request to fill it out.

The first part of the survey asks students why they attended the meetings and if they had any prior experience in cybersecurity. In the second part, students are asked to self-assess their competences on different topics before and after the training. Finally, the students are asked whether they might be interested in other cybersecurity activities in the future.

In Edition18 we received answers from 36 students (e.g., slightly less than 50% of the students attending meetings until the end of the course): 5 declared that the CTF was mandatory for them, 23 declared to be interested in the subject, and 8 selected both answers. Hence, for 13 respondents (36%) the activity was mandatory. More than half of the respondents declared they had no previous experience in cybersecurity.

In Edition19 the number of respondents was 49 (e.g., around 65% of the students attending the last meetings) and the number of students enrolled in the Computer Security course was much higher, counting for 65% of the sample. A much higher percentage of respondents (73.5%) declared no previous experience in cybersecurity.

4.1. Research question RQ1, non-formal training and competences

The first research question is: “How much does hands-on training improves the students’ Cyber-security skills?”

To answer it, we asked students to self-evaluate their competences *Before* and *After* the training using a 5-point Likert scale (see questions Q3 and Q4 in Appendix A.1). Figure 1 compares the mean values; the trend is similar in the two editions. Table 2 in Appendix A.2 reports all mean and median values.

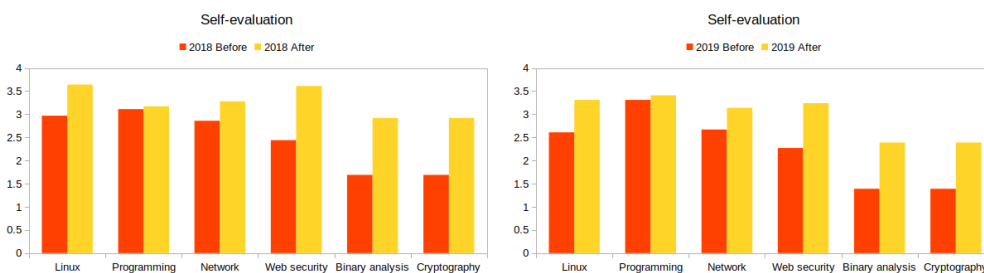


Figure 1: Mean values for students self-evaluation Before and After the training

⁴We will use Edition18 and Edition19 in the text to denote the last two editions of the project, running in 2018 and 2019, respectively.

Interestingly, *Programming* gets the lowest increment in both editions and this might be explained by the fact that the students already had experience in programming before starting this training. On the other hand, *Cryptography*, *Binary analysis*, and *Web security* get the highest increments. These were new topics for the majority of the students and they probably felt they learned a lot.

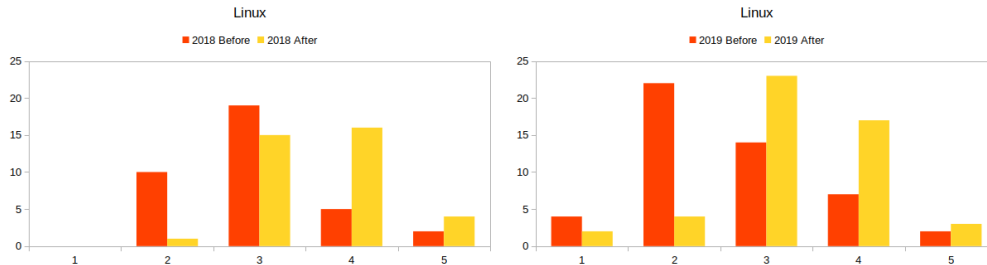


Figure 2: Linux: self-evaluation Before and After the training

Figure 2 shows the distributions of the results for *Linux* answers. An increment after the training can be observed in both editions, as all the yellow bars of the histograms are translated to the right part (e.g., higher values) of the x-axis. For *Binary analysis*, the increment is much more evident. Before the training, there is a sort of exponential decay in the results with the majority of the respondents declaring an initial weak knowledge of the subject (see orange bars in Figure 3) while, after the training, the histograms are shifted to the right and closer to normal distributions (see yellow bars). Appendix A.2 shows the distributions for the other topics: in all cases, increments can be observed, and this is particularly evident for *Cryptography* (see Figure 7), whose histograms are similar to those of *Binary analysis*.

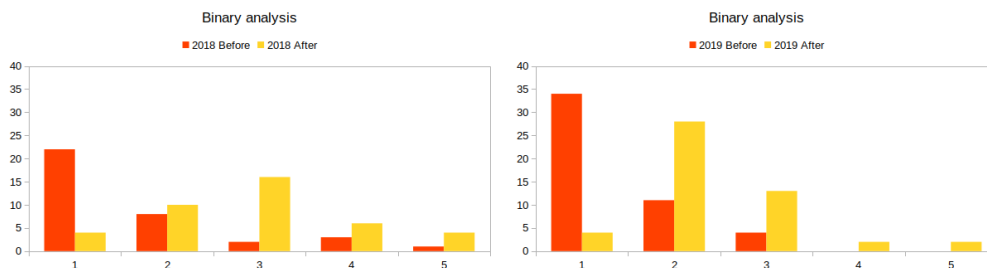


Figure 3: Binary analysis: self-evaluation Before and After the training

To summarize, research question RQ1 finds a positive answer since the respondents declared their competences improved after the training, specially for newest topics. This is less obvious for *Programming*, which is a subject students already knew before starting the training.

Table 1

Interest in Cybersecurity for Edition18 and Edition19, questions from Appendix A.1

	Edition18	Edition19
Q5 How did this training influence your opinion on:		
(a) CTF competitions (Avg)	4.083	4.082
(b) Ethical hacking (Avg)	3.072	4.082
Q6 Which other activities might be interesting for you in the future? (multiple choice)		
<input type="checkbox"/> None	7 (10.8%)	12 (17.1%)
<input type="checkbox"/> CyberChallenge.IT	13 (20.0%)	11 (15.7%)
<input type="checkbox"/> Competitive programming	12 (18.5%)	7 (10.0%)
<input type="checkbox"/> Periodic meetings to solve challenges	21 (32.2%)	21 (30.0%)
<input type="checkbox"/> Online CTFs	12 (18.5%)	19 (27.2%)
Q7 Do you think you will play other CTFs in the future?		
<input type="radio"/> Yes	16 (44.4%)	16 (32.7%)
<input type="radio"/> I would like but I have no time	9 (25.0%)	15 (30.6%)
<input type="radio"/> I do not know	5 (13.9%)	8 (16.3%)
<input type="radio"/> I would like but I am not good enough	4 (11.1%)	8 (16.3%)
<input type="radio"/> No	2 (5.6%)	2 (4.1%)
Q8 In our Master degree course, we have opened a new Cybersecurity curriculum. After this experience, would you enroll?		
<input type="radio"/> Yes	10 (47.6%)	10 (43.5%)
<input type="radio"/> No (I am interested in other topics)	1 (4.8%)	8 (34.8%)
<input type="radio"/> I do not know	10 (47.6%)	5 (21.7%)
<input type="radio"/> I cannot (I will stop after the BSc / I am already enrolled in a MSc course)	15 (-)	26 (-)

4.2. Research question RQ2, interest in Cybersecurity

The second research question is: “Does hands-on training increase the students’ interest in Cybersecurity?”

To answer it, we asked students questions Q5, Q6, Q7 and Q8 of the survey in Appendix A.1, included for readability in Table 1 along with a summary of the results.

The opinion on CTF competitions and ethical hacking (Q5) is high in both editions, with mean values larger than 4 in 3 out of 4 cases. Students also witness some interest in continuing the activities in the future (Q6). For CTFs (Q7), 16 students declared they wish playing in the future in both editions and others that they would like but have no time. If we sum these answers, we find that more than 60% of the respondents (69.4% in 2018 and 63.3% in 2019) have a positive opinion on this form of game-based learning. Question Q8 asks students if they are interested in continuing their studies in a Cybersecurity curriculum. The results are normalized without considering the last option “I cannot...” since these respondents are already enrolled in a master’s degree. Slightly less than 50% of the students declare to be interested in continuing their university careers in this field.

To summarize, the research question RQ2 finds a positive answer, but with some respondents saying they are interested in other topics.

4.3. Research question RQ3, competitive gamification as exam

The third research question is: “*Are CTF-like activities appropriate and effective for official evaluation?*”

Preparing challenges is demanding: they need to be designed, implemented, deployed on the same software configuration used during the test, and solved to check whether there are ambiguities, too much guessing, or unintended solutions. If these challenges are used in a formal exam *and* in a competition at the same time, this task is even more difficult: it requires to fix the boundaries to the topics covered during the training and to balance among “easy” challenges tailored to the theory taught in class, and more “complex” ones, specific for the competition.

In the face of this effort, how were the results of the Boeing-UniGe CTF? Did Computer Engineering students (CE in the following) perform well and pass the hands-on part of the course?

In Edition18, 71 students took part to the Boeing-UniGe CTF; 25 enrolled as CE students, 45 as Others, i.e., students for whom the CTF was not mandatory but joined the event for their personal interest. 21 out of 25 CE students (84%) solved enough challenges to pass the hands-on part of the exam, which can be considered a good result. On the other hand, only 2 CE students ranked in the top-20 positions, to witness that the vast majority of CE students expected to pass the exam, not to run for the competition.

In Edition19, 73 students attended the Boeing-UniGe CTF, 34 as CE students, 39 as Others. All the 34 CE students passed the hands-on part of the exam, and, this time, 10 students also ranked in the top-20 positions.

The results of the games were normalized in the range 0-4. A score equal to 0 means fail, and the student will have to take the exam in a following session. Values 1,2,3, and 4 mean success, and these points are added to the score obtained with the more traditional part of the exam, e.g., a written test with questions on the topics covered during official lectures.

Figure 4 shows the distribution of the points gained by CE students after the two games. Edition19 was more successful for CE students who probably were alerted by their colleagues of the previous year on this new form of evaluation. Of course, after the Boeing-UniGe CTF, other cyber exercises are organized in a standard setup, without any parallel competition, for those students who failed or could not join the event.

Figure 5 compares the results of the written test (markings ranging in [0-10]) and the results of the CTFs, to understand whether there is some correlation between these two evaluation dimensions, e.g., if students who excel in one activity also excel in the other.

Despite the small sample size, which might induce some bias, the research question RQ3 finds a positive answer. Indeed, the CTF allows us to consider some abilities that are somewhat difficult to validate with a traditional exam only. Both graphs show that a few students, particularly in Edition19, are quite good at finding vulnerabilities, but do not score so well in the theory part. On the other hand, we can see that, in particular in Edition18, some students have a reasonable grasp of the theory but lack hands-on abilities. So, to fairly evaluate the students, we need to consider both kinds of examinations.

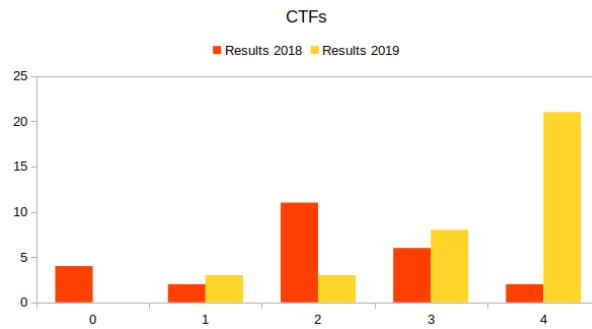


Figure 4: Students' markings after the Boeing-UniGe CTFs

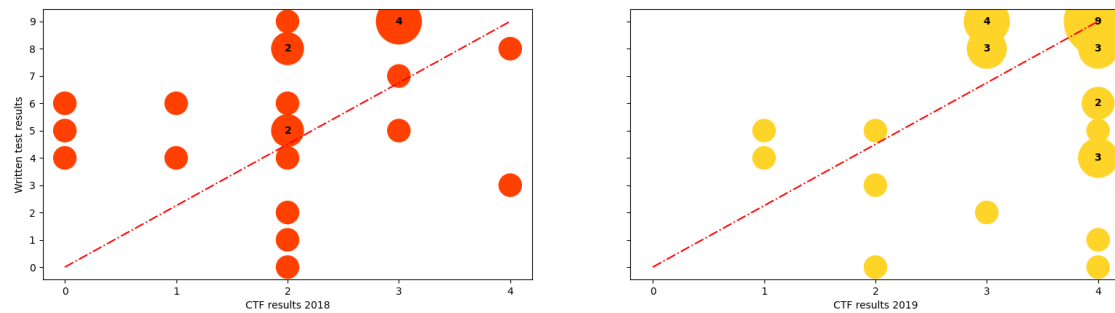


Figure 5: Markings of the Computer Security written test vs CTF results

4.4. Lesson learned

We end this section with some pros and cons we experienced and we hope the lesson learned might be useful for other instructors willing to follow a similar path.

Cons

1. The project was exciting but - especially in the first year of adoption - also very demanding. Instructors needed to prepare lectures on different topics and, in general, it is tough for a single educator to cover all of them satisfactorily. Indeed, such an experience requires the involvement of multiple people, and group collaboration is fundamental when teaching a subject that requires such different skills, not only in theory but also in practice.
2. Preparing CTF challenges for the hands-on part of an official exam can be difficult since the exercises must be tailored to the class's theory. This is precisely the opposite of what the authors of challenges do: they aim to stimulate players to always look for new solutions to unknown problems. We tried to balance these two different aspects in the CTF events we organized, but it was not easy, and, unfortunately, we left some students behind.
3. The automatic evaluation of the challenges is binary. Either the flag is correct, and the

exercise gets the full credit, or it is wrong, and the exercise gets zero credit, no matter the quality of the partial solution. If this is acceptable for a competition, some care should be taken for an exam. Therefore, some strategies should be put into practice for a partial evaluation. One possible solution is allowing students, who did not find the right flags, to write their solutions (the writeups) immediately after the game. In this way, instructors can manually evaluate them and assign partial marks when possible.

Pros

1. Some authors of this paper play in a CTF team. A side-effect of the Boeing-UniGe Scholarship Project is that some young and motivated students joined the team at the end of the training, and they still play with the senior members. Of course, this contributes to increasing the popularity of cybersecurity and ethical hacking among students. A community of young talents is growing in our department, which is probably one of the most important side-effects of this experience.

5. Conclusion

The labor market is looking for professionals in cybersecurity, and our role, as educators, is to prepare university students for their future lives at the best of our capacity. Universities have a long tradition of offering theoretical courses, but practical skills are also required in many fields, and cybersecurity is one of them. In this scenario, Capture the Flag competitions come into play since they offer a gamification environment for learning by doing, in a virtual arena that is safe, legal, live, and for some motivated students also exciting. Initially played by security enthusiasts in their spare time, these competitions are now present in more formal (academic) educational paths, starting in the US first, and reaching other countries more recently.

In this paper, we have presented a three-year project which allowed us to introduce CTFs and ethical hacking among university students, initially only in an informal context and then as part of a Computer Security class. The project reached its end, bringing (some) students closer to the world of cybersecurity competitions. We have intercepted a need, and we are persevering on this path [10] for those who have a genuine interest in pursuing a cybersecurity career.

Some tuning is necessary to learn how to develop challenges that can be used for formal exams and the problem of their binary evaluation needs to be addressed. Even though this might not be fair for a university course, it reflects what happens in the real world where software and IT infrastructures are either secure or insecure; they work or do not work.

Acknowledgments

This work was supported by the Boeing-UniGe Scholarship Project (a.y. 2017/18, 2018/19, 2019/20), which allowed us to organize on-site CTFs, and partially funded by the H2020 project “Strategic Programs for Advanced Research and Technology in Europe ” (SPARTA) and by the Italian Ministry of Defense PNRM project “UNAVOX”. The authors would also like to thank all members of ZenHack CTF team for their support.

References

- [1] L. Demetrio, G. Lagorio, M. Ribaudó, E. Russo, A. Valenza, ZenHackAdemy: Ethical Hacking @ DIBRIS, in: Proceedings of the 11th International Conference on Computer Supported Education, CSEDU 2019, Heraklion, Crete, Greece, May 2-4, 2019, Volume 1, SciTePress, 2019, pp. 405–413.
- [2] G. Vigna, The 2010 International Capture the Flag Competition, IEEE Security Privacy 9 (2011) 12–14.
- [3] D. H. Tobey, P. Pusey, D. L. Burley, Engaging Learners in Cybersecurity Careers: Lessons from the Launch of the National Cyber League, ACM Inroads 5 (2014) 53–56. URL: <https://doi.org/10.1145/2568195.2568213>. doi:10.1145/2568195.2568213.
- [4] V. Švábenský, P. Čeleda, J. Vykopal, S. Brišáková, Cybersecurity knowledge and skills taught in capture the flag challenges, Computers & Security 102 (2021) 102154. URL: <http://www.sciencedirect.com/science/article/pii/S0167404820304272>. doi:<https://doi.org/10.1016/j.cose.2020.102154>.
- [5] A. Ahmad, F. Zeshan, M. S. Khan, R. Marriam, A. Ali, A. Samreen, The Impact of Gamification on Learning Outcomes of Computer Science Majors, ACM Trans. Comput. Educ. 20 (2020).
- [6] V. Švábenský, J. Vykopal, P. Čeleda, What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences, in: Proceedings of the 51st ACM Technical Symposium on Computer Science Education, SIGCSE '20, Association for Computing Machinery, New York, USA, 2020, pp. 2–8.
- [7] J. Vykopal, V. Švábenský, E.-C. Chang, Benefits and Pitfalls of Using Capture the Flag Games in University Courses, in: Proceedings of the 51st ACM Technical Symposium on Computer Science Education, SIGCSE '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 752–758. URL: <https://doi.org/10.1145/3328778.3366893>. doi:10.1145/3328778.3366893.
- [8] A. Dabrowski, M. Kammerstetter, E. Thamm, E. Weippl, W. Kastner, Leveraging Competitive Gamification for Sustainable Fun and Profit in Security Education, in: 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15), USENIX Association, Washington, D.C., 2015. URL: <https://www.usenix.org/conference/3gse15/summit-program/presentation/dabrowski>.
- [9] M. Beltrán, M. Calvo, S. González, Experiences Using Capture The Flag Competitions to Introduce Gamification in Undergraduate Computer Security Labs, in: 2018 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE, 2018, pp. 574–579.
- [10] G. Ferraro, G. Lagorio, M. Ribaudó, Cyberchallenge.it@unige: Ethical hacking for young talents, in: Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization, UMAP '20 Adjunct, Association for Computing Machinery, New York, NY, USA, 2020, p. 127–134. URL: <https://doi.org/10.1145/3386392.3399311>. doi:10.1145/3386392.3399311.

A. Data used for the analysis

A.1. Survey administered to students at the end of the training

Q1 Why did you join the meetings on ethical hacking?	<input type="checkbox"/> It was mandatory for Computer Security <input type="checkbox"/> I was interested in the subject
------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------

Q2 Before this experience, did you attend other activities related to Cybersecurity?	<input type="checkbox"/> No previous experience <input type="checkbox"/> Curricular courses/seminars at my univ. <input type="checkbox"/> Courses/seminars outside my univ. <input type="checkbox"/> Informal meetings <input type="checkbox"/> CTF competitions <input type="checkbox"/> Other
--------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Q3 How do you evaluate your competences on the following topics before starting the training? (a) Linux, (b) Programming, (c) Network protocols, (d) Web security, (e) Binary analysis, (f) Cryptography	(1) Very poor (2) Poor (3) Average (4) Good (5) Very good
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------

Q4 How do you evaluate your competences on the following topics after the training?	See question Q3
--------------------------------------------------------------------------------------------	-----------------

Q5 How did this training influence your opinion on: (a) CTF competitions (b) Ethical hacking	(1) Very negatively (2) Negatively (3) Indifferent (4) Positively (5) Very positively
----------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------

Q6 Which other activities might be interesting for you in the future? (multiple choice)	<input type="checkbox"/> None <input type="checkbox"/> CyberChallenge.IT <input type="checkbox"/> Competitive programming <input type="checkbox"/> Periodic meetings to solve challenges <input type="checkbox"/> Online CTFs
-----------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Q7 Do you think you will play other CTFs in the future?	<input type="radio"/> Yes <input type="radio"/> I would like but I have no time <input type="radio"/> I do not know <input type="radio"/> I would like but I am not good enough <input type="radio"/> No
---------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Q8 In our Master degree course, we have opened a new cybersecurity curriculum. After this experience, would you enroll?	<input type="radio"/> Yes <input type="radio"/> No (I am interested in other topics) <input type="radio"/> I do not know <input type="radio"/> I cannot (I will stop after the BsC / I am already enrolled in a MSc course)
-------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

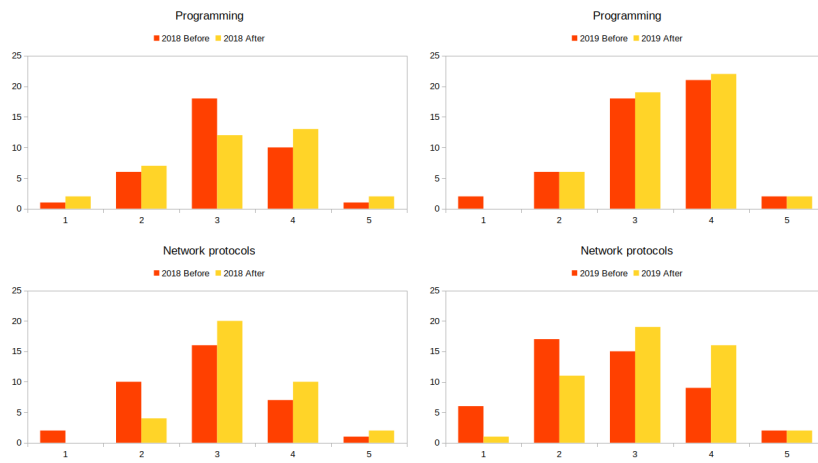
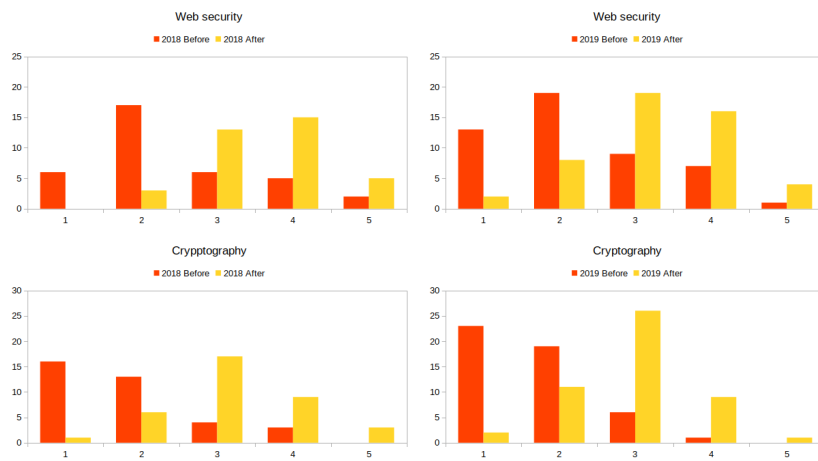
A.2. Results of self-evaluation

Summary of the results of questions Q3 and Q4 (see Table 2) and distributions of the self-evaluation results for the topics omitted from Section 4 (see Figures 6 and 7).

Table 2

Average (Avg) and median (Mdn) values for students self-evaluation Before (B) and After (A) the training

Topic	Edition18				Edition19			
	Avg _B	Avg _A	Mdn _B	Mdn _A	Avg _B	Avg _A	Mdn _B	Mdn _A
Linux	2.97	3.64	3	4	2.61	3.31	2	3
Programming	3.11	3.17	3	3	3.31	3.41	3	3
Network protocols	2.86	3.28	3	3	2.76	3.14	3	3
Web security	2.44	3.61	2	4	2.26	3.25	2	3
Binary analysis	1.69	2.92	1	3	1.39	2.39	1	2
Cryptography	1.83	3.19	2	3	1.69	2.92	2	3

**Figure 6:** Programming and Network protocols: self-evaluation Before and After the training**Figure 7:** Web security and Cryptography: self-evaluation Before and After the training