# ZenHackAdemy: Ethical Hacking @ DIBRIS

Luca Demetrio, Giovanni Lagorio, Marina Ribaudo, Enrico Russo and Andrea Valenza
*DIBRIS, University of Genoa, Italy*

Keywords: Ethical Hacking, Capture the Flag Competitions, Non-formal Learning.

Abstract: Cybersecurity attacks are on the rise, and the current response is not effective enough. The need for a competent workforce, able to face attackers, is increasing. At the moment, the gap between academia and real-world skills is huge and academia cannot provide students with skills that match those of an attacker. To pass on these skills, teachers have to train students in scenarios as close as possible to real-world ones. Capture the Flag (CTF) competitions are a great tool to achieve this goal, since they encourage students to think as an attacker does, thus creating more awareness on the modalities and consequences of an attack.
We describe our experience in running an educational activity on ethical hacking, which we proposed to computer science and computer engineering students. We organized seminars, outside formal classes, and provided online support on the hands-on part of the training. We delivered different types of exercises and held a final CTF competition. These activities resulted in growing a community of students and researchers interested in cybersecurity, and some of them have formed ZenHack, an official CTF team.

## 1 INTRODUCTION

Cybersecurity attacks, causing data breaches and failure of critical systems and infrastructures, are on the rise. For instance, a recent one targeted private data on German Chancellor Angela Merkel and other senior German lawmakers and officials[1]. As a counterpart to the number and complexity of attacks, there is the need for a competent workforce to prevent or mitigate such threats. A *hacker* is a computer expert, who tries to understand how systems operate and communicate over a network, how they are designed and how they are protected, whether they are vulnerable, and so on. When these activities are performed under the proper authorization, this expert is called *ethical hacker* (or *white hat hacker*). Instead, when an expert uses the same skill set maliciously, they are usually called *black hat hacker*.

Ethical hackers possess multiple and diversified technical skills and, according to Bratus (Bratus, 2007), standard computer science and computer engineering curricula lacked several topics for building such expertise. This shortage led to unrealistic teaching environments that were far from the real world's actual complexity, creating false expectations in students and causing problems when, after graduation, they joined professional arenas, where security was vital to many companies. Another critical point to teach students how to hack is the introduction of ethical and legal implications of hacking others' machines, services, or networks, and the implications of misusing their skills (Pashel, 2006).

This alarming lack of skills is still present today, despite we live in the digital and always connected world, which requires an experienced and educated workforce ready to fill the thousands of open cybersecurity roles across the globe[2].

Outside of academia and official certification bodies, the practice of ethical hacking has received much attention in recent years. Many corporations organize training programs for their employees to teach them how hackers think and work, to prevent future breaches. Moreover, the last decade also saw the growth of worldwide cybersecurity competitions, which span over many aspects of computer science, information technology and security education. A good starting point to get an idea of the number and quality of such competitions is the website CTFtime[3] that continually updates a list of the past, current and future events. Thanks to this lively *online gym*, recent literature (see for instance (Conti et al., 2011)) suggests to include some form of competitions in se-

[1] https://techcrunch.com/2019/01/04/germany-data-breach-lawmakers-leak/

[2] See for example cybersecurityventures.com/jobs

[3] https://CTFtime.org



Demetrio, L., Lagorio, G., Ribaudo, M., Russo, E. and Valenza, A.
ZenHackAdemy: Ethical Hacking @ DIBRIS.
DOI: 10.5220/0007747104050413
In *Proceedings of the 11th International Conference on Computer Supported Education (CSEDU 2019)*, pages 405-413
ISBN: 978-989-758-367-4

curity education programs, to engage students with hands-on using real-world security practices.

In 2014 the European Union Agency for Network and Information Security (ENISA) started to organize a yearly *European Cyber Security Challenge*, which is an initiative that aims at enhancing cybersecurity talent across Europe and connecting high potentials with industry-leading organizations [4].

Unfortunately, changing the topics taught in a university curriculum is not always an easy task, since curricula are often the result of much different balances and mediation among faculty members. However, triggered by the success of these online competitions, in 2017 we introduced some hands-on activities, outside the formal classes, and offered *non-formal* meetings on ethical hacking to expose our students to new trends and directions.

We distinguish between formal and non-formal learning according to the following definitions: *formal learning* is official, structured, organized by public or private organizations and ends with formal certification (e.g., university credits); on the other hand, *non-formal learning* is any structured and organized learning which does not lead to a formal level of qualification.

This paper reports on a non-formal educational activity, discussing student recruitment, training organization, communication management, and some results we achieved. To assess our results we defined the following research questions:

*RQ1 "How much did this non-formal training impact on the competences of our students?"*

*RQ2 "Did this non-formal training increased students' interest toward cybersecurity and ethical hacking?"*

and, at the end of the training, we administered a short survey, to collect some preliminary feedback.

The rest of the paper is organized as follows: Section 2 provides the context, by briefly introducing CTF competitions. Section 3 is the core of this work and describes the ethical hacking activities carried on in our department. Section 4 reports the results of the survey and some feedback. Section 5 presents some related work and, finally, Section 6 concludes and sketches some ideas for future activities.

## 2 CAPTURE THE FLAG

*Capture the Flag (CTF)* is a special kind of information security competition and different types of CTFs exist, among them: *jeopardy*, *attack/defence*, and mixed.

Jeopardy competitions involve multiple categories of challenges, each of which contains a vulnerability. Participants, often grouped into teams, must exploit these vulnerabilities to find hidden *flags*, that is, strings in a given format. The knowledge of a flag proves that the corresponding challenge, to be precise its vulnerability, has been successfully exploited. Participants (teams) do not directly attack each other but usually enroll into an online platform where they find the challenges and submit their flags to gain points. Competitions in this format allow students to think *adversariarly*, i.e., to think as an attacker would, and this form of gamification motivates them to learn by doing.

Jeopardy CTFs have a fixed duration, which is usually from one to a few consecutive days. Online support is provided during the contest by using online team collaboration tools such as Slack[5] or Discord[6]. A dynamic scoreboard shows the progress of the contest, listing the teams and their scores. At the end of the competition the scoreboard is frozen, and the top three teams are listed as winners on the CTFtime website.

Each CTF competition has a given rate, depending on its reputation and quality, and each team gets a score based on the obtained points and the competition rating. This procedure permits to compute a global rating among all teams that took part in at least one competition. The interested reader may find the current ratings on the CTFtime website[7].

In attack/defense CTF teams run an identical machine, or a small network, injected with vulnerable services. In this case, the goal of each team is to find and exploit the vulnerabilities in opponent' machines, while fixing or mitigating flaws in their own. Compromising a machine enables a team to acquire hidden flags. Note that, differently from jeopardy CTFs, in this case, the flags change during the event because a *scoring bot* service updates them regularly, and teams lose points if their services are not up when the scoring bot contacts them. That is, *availability* of services takes an important role in calculating the final score.

Usually, teams have a couple of hours to understand the playing scenario before the competition starts. Although attack/defense CTFs are more demanding to play, they allow participants to gain experience with both offensive and defensive related skills.

Finally, mixed competitions may have different formats. For instance, *Build-it/Break-it/Fix-it*

[4]https://www.europeancybersecuritychallenge.eu/

[5]https://slack.com/

[6]https://discordapp.com/

[7]https://ctftime.org/stats/

(BIBIFI) competitions (Ruef et al., 2016) ask build-it teams to write software, which is subsequently attacked by break-it teams. BIBIFI contests consist of three phases. The first one, *build-it*, asks small development teams to build software according to a given specification that includes security goals. The second phase, *break-it*, asks teams to find defects in other teams' submissions. Reported defects benefit the break-it team's score and penalize the build-it team's score. The final phase, *fix-it*, asks builders to fix bugs and thereby get some points back.

In all types of competitions, there is also a follow-up phase dedicated to the publication of *write-ups*. Who solved a given challenge can write a short post, detailing the steps they followed. Then, authors can also ask the CTFtime website to host their write-ups.

From an educational point of view, this is extremely useful since, on the one hand, it allows participants to arrange and summarize the steps towards their solutions and, on the other hand, it allows to compare different techniques, chosen by different people, to face the same problem. Write-ups are even more useful for those who did not succeed in solving some exercise since they can, a-posteriori, find hints valuable for future competitions.

# 3 THE ZenHackAdemy

The dialect name of Genoa is *Zena*; since we organize activities on ethical hacking, we (see 3.1) coined the name ZenHackAdemy for such training, by combining the words *Zena*, *Hacking*, and *Academy*.

## 3.1 Who and Why

We are a group of researchers working in cybersecurity, who discovered CTFtime through word of mouth. After attending some online jeopardy competitions, we immediately realized the educational potential of this type of activity. At the same time, we also realized that during our studies we were never exposed to lectures or practical activities that would have enabled us to solve the proposed challenges. So, we thought to offer undergraduate students some hands-on activities to fill this gap. Hence, we rolled up our sleeves, deepened our knowledge in the practical aspects and tools, and started participating in online competitions.

As already said in Section 1, modifying the content of official curricula is a difficult and time consuming process so, in October 2017, we decided to assess the real interest in these topics by starting some non-formal training, outside official lectures, to get some feedback from motivated students, interested in acquiring some practical skills that formal training did not offer. The first step was the advertising and organization of a two hours presentation, during which we launched a call for participation to the *unofficial* events on Ethical Hacking @ DIBRIS.

## 3.2 Autumn 2017, First Pilot

The attendance to the first presentation was noticeable, confirming our suspicions that there was indeed much interest in these kinds of activities and therefore we defined a calendar of weekly meetings. We scheduled Friday afternoon as meeting day to maximize the participation, since it was the only slot without official courses.

During each meeting we covered a different topic, ranging from web security to binary analysis, from network analysis to cryptography. After some theory, each seminar was accompanied by exercises proposed to students during the class as well as homework.

Despite the unfavorable placement in the week, participation was somewhat 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 an on-site Jeopardy CTF event. Thanks to a grant offered by Boeing Company, we could also offer two prizes for the best-performing students.

The platform chosen for hosting the local CTF is *CTFd*[8], an open source software designed to support CTF organizers. Such a platform handles publication of exercises, participant enrolments, and flag submissions. Moreover, CTFd allows organizers to define two types of scoring: *static*, that is, the score of each challenge is defined a-priori before the competition starts, and *dynamic*, where each challenge has an initial score, which decreases during the competition according to the number of submitted solutions. Hints can be associated with challenges, this is especially useful for the hard ones, and participants can decide whether to read them or not; reading a hint has a cost, e.g, some points are deducted.

32 students attended the first on-site CTF that lasted for 5 hours and exposed them to exercises on different categories. The winner was a 2nd-year bachelor student in Computer Engineering with no prior experience in computer security; the second classified was 1st-year master student in Computer Science, who just attended his first course on security during the same semester. Even though numbers may not seem striking, a small seed was planted, introducing

[8]https://ctfd.io/

awareness of this kind of non-formal learning among students interested in the topic. Moreover, as a major result, some strongly motivated students joined us in the ZenHack team and we still meet, train and take part into many online events advertised on CTFtime.

### 3.3 Autumn 2018, Second Edition

At the beginning of the academic year 2018/19 we re-proposed the activity described in previous section, this time with greater confidence and competence with respect to the first pilot.

**Students Enrollment.** In October 2018, once again, interested students were invited to a plenary session during which the winners of the first CTF, and new members of the ZenHack team, introduced themselves, presented some exercises they solved, and some lessons they learned by finding the exploits.

Then, we launched a new call for participation for a 10-week non-formal training, reaching a larger number of students w.r.t. the first pilot. To be precise, in this academic year students attending the Computer Security course have been invited to join lectures since the course holder recognized the importance of such hands-on activities and decided to add this non-formal training as part of the official course. On average, in this second edition, 80 participants showed up during the weekly meetings, mixing students of the Computer Security course with students interested in the subject and involved on a voluntary basis; we use *elective* students to identify this latter group. As a result, teaching activities were both formal and non-formal, depending on the group each student belongs to, and this choice made things more difficult as we detail in Section 4.

**Lectures Organization.** Activities started on October 2018, according to the schedule shown in Table 1. In this second edition, all exercises were published on a CTFd instance dedicated to the training so that students could practice with the platform from the beginning of the learning path.

Table 1: Calendar of the activities, Autumn 2018.

| | |
|---|---|
| 12/10 | Ethical hacking and Linux basics |
| 19/10 | Network protocols and Wireshark |
| 26/10 | Web security (client) |
| 09/11 | Basics on machine learning |
| 16/11 | Basics on cryptography |
| 23/11 | Exercises |
| 30/11 | Web security (server) |
| 07/12 | Binary analysis |
| 14/12 | Binary analysis (cnt.) |
| 20/12 | Final on-site CTF |

After a general, but fundamental, introduction on the importance of *ethics* and *legislation*, when practicing ethical hacking, we presented the basic Linux commands since this is the operating system generally used to solve this type of challenges. Exercises labelled as *Misc* closed the teaching of the first day. Misc stands for *miscellaneous* and exercises in this category are always present in Jeopardy CTF competitions: they are introduced to test participants generic skills, which can be classified as *lateral thinking*.

The subject of the second meeting was network security and forensics. In the first part we reviewed some basics of networking, focusing on the TCP/IP stack, addressing, and protocols. In particular, these topics were the fundamentals to learn how to use Wireshark[9], a mainstream network protocol analyzer. The aim was learning how to understand traffic flows, filter interesting packets, decode and read payloads, and extract artifacts. Hence, in the second part, we provided students with some network traffic captures to be analyzed.

We scheduled two meetings on web security due to the importance of the topic. The first meeting focused on client-side web security, to expose students to vulnerabilities like Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) and Cross-Site Script Include (XSSi). This seminar showed the importance of client-side security, which is often neglected in favor of server-side security. For each of the vulnerabilities above, students performed attacks on the Google Gruyere[10] platform. The second meeting was on server-side security, focusing on vulnerabilities such as SQL Injection (SQLi) and Directory Traversal. SQLi was inspected in depth by starting from a simple login bypass, then diving into Union-based SQLi, Error-based SQLi and Blind SQLi. Students could find and exploit these vulnerabilities on a custom built website, thus simulating a real penetration testing session.

In this edition we decided to cover also some basics of machine learning, particularly an introduction to *adversarial* machine learning (Huang et al., 2011). We introduced a practical threat against machine learning algorithms by showing one of the most famous attacks taken from the state-of-the-art (Goodfellow et al., 2014). We provided the students with challenges that covered the key concepts of the proposed attack, as our goal was to teach them how to fool a simple classifier and, as a consequence, to ma-

[9]https://www.wireshark.org/

[10]https://google-gruyere.appspot.com/

nipulate the mathematical objects that characterize every machine learning algorithm.

Math background is fundamental to solve real challenges, and therefore one of the meetings was on cryptography and introduced some topics the students of Computer Security already met during the course, while electives did not.

Reverse engineering binary code is the backbone of vulnerability and malware analysis in all contexts where source code is not available; for instance, when studying and/or securing untrusted or proprietary code. So, we devoted the last two meetings to a brief introduction to binary reversing of Linux executables. The first meeting covered executable "lifecycle", that is, how binaries are linked and loaded; we briefly discussed the ELF file format and the tools to statically analyze it. Then, we covered the disassembly process and why it can be trickier than one might initially think (e.g., overlapping instructions and opaque predicates). In the second meeting we covered the cornerstone of reverse engineering binaries, by using the static analysis tools discussed before, and by leveraging some tools for dynamic analysis, ranging from tracing tools, like *strace* and *ltrace*, to full-fledged debuggers like *gdb* and *radare2*. In particular, we solved some introductory "crackmes", the *IOLI crackmes*[11], and a couple of simple CTF challenges, chosen from the ones offered by previous CTFs we participated to.

Finally, in week 10 we organized the on-site CTF that will be described later.

All meetings were streamed using YouTube and afterward published for the students who could not attend. We weekly published, on our instance of CTFd, some hands-on exercises; 126 students registered to the platform, and 90 (e.g., around 70%) were effectively active and tried to submit some flags.

Notice that all topics covered during the meetings are mainstream in ethical hacking, and they cover some of the real attacks that industries and governments have to deal with. The same topics fit well into categories that are found in online challenges. If the instructors do not have their own set of exercises to propose to students, they can take advantage (and in some cases we did as well) of many open resources available on platforms for this specific type of education; the so-called *war games*, such as OverTheWire[12], W3Challs[13], and Hack This Site[14]. We used them for some challenges and suggested their use to motivated students for individual training.

**Communication Management.** We set up a Telegram channel to communicate with this heterogeneous group and we used it to announce the meetings on a weekly basis, and to share slides and other material. We also advertised the participation to online CTFs for those students willing to get a grasp of the worldwide competitions community.

**On-site CTF.** On December 20th 2018, we organized a 4 hours on-site CTF, again supported by a grant offered by Boeing Company. This year we decided to have four prizes of a smaller entity, to reward a larger number of students. Out of the 90 students active on the training platform, 71 (79%) took part to the local CTF, 22 enrolled in the Computer Security course, the other 49 as elective students. We prepared 21 exercises, in all categories introduced during the training. In order to meet the dual role of this year's CTF, e.g., a competition among students for a grant and the hands-on part for the Computer Security exam, challenges were of two different types. Seven of them, labeled with a "*" (star), were specific for the exam. Their score was static and low (only 10 points each). All remaining, more difficult, exercises used dynamic score, which is the current trend of online competitions; their score started from 500 points, and it was decremented with each new submitted solution.

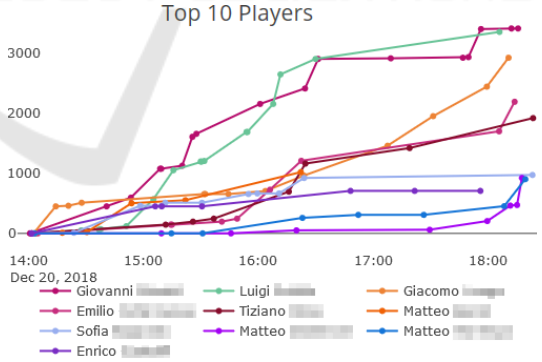


Figure 1: Final scoreboard.

Figure 1 shows the final scoreboard, with the top 10 participants and their progress during the CTF. Below the curves, a list participant names and their respective scores are also available but omitted from the image. Interestingly, 3 out of top 4 winners belong to the group of elective students, who followed the training path because they were genuinely interested. Similarly, when considering the top 10 participants, 9 out of 10 are elective. Computer Security students, for whom the training was not optional, did not perform

[11] https://github.com/Maijin/Workshop2015/tree/master/IOLI-crackme

[12] https://overthewire.org/wargames/

[13] https://w3challs.com/

[14] https://www.hackthissite.org/

as well as elective students, that chose to attend because of their passion. This result might seem obvious; what surprised us was the apparent lack of passion among Computer Security students.

## 4 RESULTS

To answer the two questions *RQ1* and *RQ2* of the Introduction, we administered a short anonymous survey consisting of multiple choice questions, 5-point scale questions, and a final open-ended question for any feedback (see the Appendix for the complete survey).

The survey was announced to students via Telegram after the CTF, along with a request to fill it out, and with a message clearly stating we were collecting information related to the ZenHackAdemy activities only, to avoid confusion with the Computer Security course[15]. We received 36 responses, that correspond to the 40% of our sample, considering the 90 active students on the training platform.

The first question of the survey, Q1, asks students why they attended ZenHackAdemy activities and proposes two different answers: 1) *mandatory*, for Computer Security students, and 2) *interested in the topic*, for all the students. Respondents could select both answers, and 13 (36%) of them declared to be Computer Security students, but 31 out of 36 (86%) selected the second option, and therefore the majority of the students, for which the training was mandatory, would have probably followed it also as elective students. This result is contrasting with the scoreboard of the on-site CTF.

Concerning background of respondents, 20 (55%) did not have any prior experience in the field. 31 out of the 36 (86%) respondents participated in the on-site CTF, and 16 (44%) declare they will participate to other CTFs in the future, 9 (25%) would like, but they have no time, only 2 declare they will not.

To answer *RQ1* we formulated the two questions Q3 and Q4 written in the Appendix. Figure 2 shows on the top how participants self-evaluated themselves on different topics, based on their prior knowledge, and, on the bottom, their self-evaluation on the same topics after the training. By comparing the two pictures, it is clear that there is an overall improvement concerning the skills of the participants. In particular, we observe that there is a shift towards an *average* or *good* level of self-evaluation (the intensity of blue becomes darker), and less participants declare to know nothing (*none*) on the topics proposed in the list.

[15]At the end of each semester, all students are asked to fill in surveys on the official courses they attended.

From the results, we also noticed that few students self-evaluated themselves worse after the training. We think they understood they might have overrated their skills; hence, the meetings provided a sort of "reality check" for them.

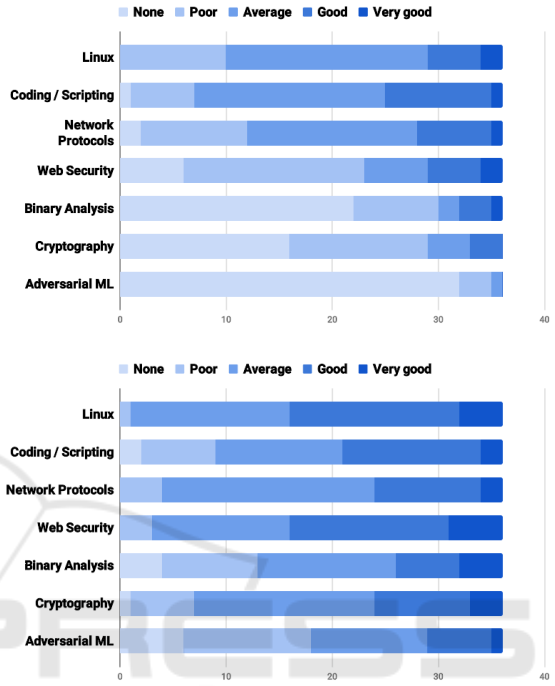


Figure 2: Students self-evaluations before the training (top) and after the training (bottom). Topics: *Linux, Coding/scripting, Network protocols, Web security, Binary analysis, Cryptography, Adversarial machine learning.*

To answer *RQ2* we proposed question Q9 (see the Appendix) and Figure 3 shows the answers, highlighting an overall positive impression on the topics, with a particular focus on ethical hacking, as it is the only topic without any negative vote. As regards the other topics, we think that the negative scores given to the challenges are due to the fact that these tasks may be frustrating for beginners, as the learning curve is steep. Moreover, we got complaints about the difficulties encountered with mixed audience meetings, that is meetings for both elective and Computer Security students; this negatively impacted on the survey's answers.

To summarize, for *RQ1* we can indeed claim that the non-formal meetings of the ZenHackAdemy allowed students to improve their skills: some learned new concepts, others improved their prior understanding. For *RQ2*, we can observe that participants' opinions regarding cybersecurity-related topics are rather positive, even though many of the respondents did not have any prior knowledge or experience in the field.

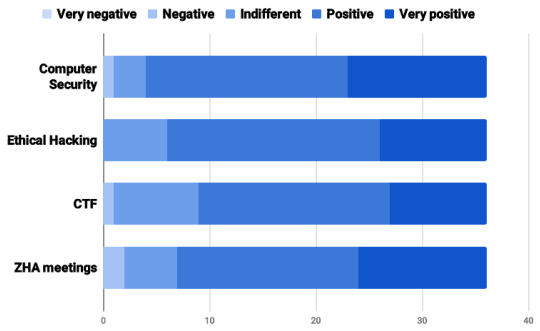


Figure 3: Students' opinions on *Computer Security, Ethical Hacking, CTF, ZenHackAdemy meetings*.

**Preliminary Feedback.** In the last open-ended question of the survey some respondents left positive comments, others wrote suggestions for the next edition. We list here some comments that highlight critical issues we need to address.

One of the respondents suggests to *"Increase individual assistance, if possible."* Unfortunately, instructors work on a voluntary basis, and it is difficult, if not impossible, to provide individual training to less skilled students, especially when the size of the class increases, like it happened in the second edition.

Another respondent observes that *"Exercises of the final CTF were too difficult."* This is only partially true since there were exercises of different difficulty levels. Being a competition for a scholarship, we also introduced difficult exercises; it was part of the game.

A third comment suggests to *"Improve the collaboration with the professor responsible for the Computer Security course since students enrolled in the course were too worried about the exam to appreciate the competition."* As a matter of fact, mixing two groups of students of different ages, with different skills and, mostly, with different motivations, represented a real problem and we need to address it in the future.

## 5 RELATED WORK

The USENIX Workshops on Advances in Security Education constitutes an important venue to share educational experiences in the field of cybersecurity. Indeed, the workshops' papers introduce several case-studies on educational activities similar to ours. In many cases, gamification methodologies and techniques were selected to present cybersecurity scenarios, asking students to find possible solutions.

For instance, (Morelock and Peterson, 2018) reports on a 10-week experience during which students played an Alternate Reality Game, presented with a realistic narrative: *"The daughter of a student expelled 20 years ago is back to her father's campus to avenge him, and her initial point of attack is the website of a security course..."*. A goal of the experience was to understand key concepts of cybersecurity threats and to improve students' skills and abilities to prevent cyber attacks. Results show that after the course students positively changed their perception of the cybersecurity profession, in terms of understanding the tasks and problems that need to be solved.

(Chothia and de Ruiter, 2016) discusses an 11-week course addressing IoT security. Like in our case, each week presents a single topic, such as network protocols, web security, reverse engineering. During the course, students discovered a large number of vulnerabilities hidden inside the devices under analysis, and they learned how to carry on penetration testing activities on a set of unknown devices and programs. Another paper (Chothia et al., 2017), of the same research group, proposes an experiment based on gamification. During an 11-week cybersecurity course, students played the role of new hired IT security employees in charge of different tasks, presented as CTF-like exercises. Each exercise offers the chance of choosing different options for advancing into the plot of the game. Depending on what the students decide, the plot evolves and changes accordingly. Authors state that those students who actively followed the narration offered by the game scored better, as opposed to those who ignored the suggestions.

The goal of (Vykopal and Barták, 2016) is to understand the impact of the hints and the solutions given to the students who approach cybersecurity challenges. Actions performed by the students on the training platform were logged, producing data that were later analysed. Results show that there was no evident correlation between the success rate of a challenge and the hints provided.

Flushman et al. (Flushman et al., 2015) set up a 10-week course, split into different modules. Each module covers a different cybersecurity topic. Students are organized in groups of four, mimicking a regular CTF team, and they play an Alternate Reality Game. Each exercise is provided with a fictional situation, blurring the boundary between the challenge and the inspired real-life scenario. At the end of each challenge, students are asked to reflect on their individual experience: these data have been used by the organizers to monitor the behavior of the participants and to discover problems into the hosting platform. Like in our experience, results show how gamification improved students' performances and awareness of computer security.

# 6 CONCLUSIONS

Cybersecurity professionals work in different contexts such as networks, operating systems, IoT, databases, and they must have a deep knowledge of a variety of tools and programming languages to manage such complex, heterogeneous set of environments. Hands-on training is a must for such a profession, but traditional university courses often lack these practical activities. In those scenarios, other types of activities, such as cybersecurity competitions, can be proposed to motivated students, as we did with the ZenHackAdemy.

After two years of experience, we can claim that, despite being perceived as a difficult subject, practical training attracts strongly motivated students. Moreover, we can state that these activities raised the awareness of students towards different aspects of the broad world of Computer Security.

The answers to question Q11 "*In our Master degree we are planning a new cybersecurity curriculum: after this experience, would you enroll?*" were: Yes, 10 (28%); No 1 (3%)1; I do not know, 10 (28%); I cannot, 15 (41%). By looking at these answers, and thanks to the general success of the activities we proposed, we will finally open a new curriculum, starting from the next academic year, with new official courses in this field. Premises are encouraging.

# ACKNOWLEDGEMENTS

This work was partly supported by Boeing company: the Boeing-Unige Scolarship Project 2018 funded students scholarships.

# REFERENCES

Bratus, S. (2007). What hackers learn that the rest of us don't: Notes on hacker curriculum. *IEEE Security Privacy*, 5(4):72–75.

Chothia, T. and de Ruiter, J. (2016). Learning From Others' Mistakes: Penetration Testing IoT Devices in the Classroom. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*, Austin, TX. USENIX Association.

Chothia, T., Holdcroft, S., Radu, A.-I., and Thomas, R. J. (2017). 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 (ASE 17)*, Vancouver, BC. USENIX Association.

Conti, G., Babbitt, T., and Nelson, J. (2011). Hacking competitions and their untapped potential for security education. *IEEE Security Privacy*, 9(3):56–59.

Flushman, T., Gondree, M., and Peterson, Z. N. J. (2015). This is Not a Game: Early Observations on Using Alternate Reality Games for Teaching Security Concepts to First-Year Undergraduates. In *8th Workshop on Cyber Security Experimentation and Test (CSET 15)*, Washington, D.C. USENIX Association.

Goodfellow, I. J., Shlens, J., and Szegedy, C. (2014). Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*.

Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., and Tygar, J. (2011). Adversarial machine learning. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, pages 43–58. ACM.

Morelock, J. R. and Peterson, Z. (2018). Authenticity, ethicality, and motivation: A formal evaluation of a 10-week computer security alternate reality game for CS undergraduates. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*, Baltimore, MD. USENIX Association.

Pashel, B. A. (2006). Teaching students to hack: ethical implications in teaching students to hack at the university level. In *InfoSecCD*.

Ruef, A., Hicks, M., Parker, J., Levin, D., Mazurek, M. L., and Mardziel, P. (2016). Build it, break it, fix it: Contesting secure development. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 690–703, New York, NY, USA. ACM.

Vykopal, J. and Barták, M. (2016). On the design of security games: From frustrating to engaging learning. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*, Austin, TX. USENIX Association.

# APPENDIX

| | | |
|---|---|---|
| Q1: | Why did you join ZenHackAdemy activities? | ☐ It was mandatory for Computer Security<br>☐ I was interested in the subject |
| Q2: | Before this experience, did you attend other activities related to cybersecurity? | ☐ No previous experience<br>☐ Curricular courses/seminars at my university<br>☐ Courses/seminars outside my university<br>☐ Informal meetings with ZenHack<br>☐ CTF competitions<br>☐ Other |
| Q3: | How do you evaluate your competences on the following topics before starting the ZenHackAdemy activities? *(a) Linux, (b) Coding/scripting, (c) Network protocols, (d) Web security, (e) Binary analysis, (f) Cryptography, (g) Adversarial machine learning* | (1) None<br>(2) Poor<br>(3) Average<br>(4) Good<br>(5) Very good |
| Q4: | How do you evaluate your competences on the following topics after attending the ZenHackAdemy activities? | See Q3 |
| Q5: | Which activities do you consider more useful to learn cybersecurity and ethical hacking? | ☐ ZenHackAdemy meetings<br>☐ Videos of ZenHackAdemy meetings<br>☐ Training on ZenHackAdemy platform<br>☐ Other videos on cybersecurity<br>☐ Training on other websites (i.e., W3Challs)<br>☐ Posts / write-ups with solutions<br>☐ Individual participation to CTFs |
| Q6: | Did you attend the CTF on Dec. 20? | ◯ Yes ◯ No |
| Q7: | If Yes, how do you evaluate the following aspects of the CTF? *(a) Organization, (b) Presentation, (c) Challenges, (d) T-shirt* | (1) Very negative<br>(2) Negative<br>(3) Indifferent<br>(4) Positive<br>(5) Very Positive |
| Q8: | Will you participate in other CTFs in the future? | ◯ Yes<br>◯ I would like, but I do not have time<br>◯ I do not know<br>◯ I would like, but I do not have enough skills<br>◯ No |
| Q9: | How did ZenHackAdemy activities influence your opinion on: *(a) Computer Security, (b) Ethical Hacking, (c) CTF, (d) ZenHackAdemy meetings*? | (1) Very negative<br>(2) Negative<br>(3) Indifferent<br>(4) Positive<br>(5) Very Positive |
| Q10: | Which ZenHackAdemy activites might be interesting for you in the future? | ☐ None<br>☐ Competitive programming<br>☐ Periodic meetings to solve challenges<br>☐ Online CTFs with ZenHack team |
| Q11: | In our Master's degree course, we are planning a new cybersecurity curriculum. After this experience, would you enroll? | ◯ Yes<br>◯ No<br>◯ I do not know<br>◯ I cannot (I will stop after the bachelor's / I am already enrolled in a Master's degree course) |
| Q12: | If you want, you can leave a comment | |