we also observed more interaction among the instructors and the class, and among the students themselves, even though none of us ever met in person.

Moreover, some of the more motivated students, once they acquired some initial skills, enrolled in online CTFs, specifically organized for beginners. This active approach allowed them to keep learning beyond the hours provided by the project. These episodes are a point in favor of the activity we are carrying out: students are motivated, they appreciate the covered topics, and they are committed despite the objective difficulties of this period. And it is also a source of satisfaction for us, who dedicate many hours to CC.IT, outside our institutional teaching load.

Of course, the project also has some weaknesses, at the organizational and educational level. The high number of training nodes, and registered students, highlighted some scalability problems, which have been partially addressed.

The software platform used to automate the scoring of submissions during the admission phase was a great addition, but it needs some improvements. For example, there was no possibility of withdrawing early from the test. Given the distributed nature of the admission phase, which is like an exam, but with thousands of students spread in dozens of labs around the country, it is essential to let each node manage some issues locally, as the entrances and exits from the labs. This functionality, which is implemented for the next edition, was missing, and a large number of messages was exchanged between universities and the central organization.

A lot of effort has gone in preparing the syllabus and support materials (slides and accompanying videos, plus challenges and their detailed write-ups) for the CC.IT project. However, notwithstanding this enormous work, each node has its peculiarities, strengths, and weaknesses. For instance, some local instructor might be an expert of, say, web security, but not so skilled in cryptography. And, while the supporting material helps, it takes dedication and a lot of work to prepare engaging and technically adequate lectures on such disparate topics. Furthermore, we cover a lot of ground in (relatively) few weeks. It is challenging to find the right amount of theory versus practice. On the one hand, with too much theory then students can not tackle any practical challenge. On the other hand, you cannot understand how to use the tools without a reasonable background effectively. So, choosing the specific topic to deepen is a work still in progress and, in some sense, a moving target, which depends on the class and its varied background.

This diversity among topics is another reason why creating a local community pays back in the long run. The nodes that have an active CTF team, in our case *ZenHack*, can count on its members for supporting the new students and explain some rather specific topic or technique. Their experience is invaluable, and it makes the difference in bridging the gap between theory and practice.

As we discussed in Section 4.3, selecting the students with the right mindset and skills is very though. While some programming abilities are necessary, excelling in programming challenges does not imply excelling in cybersecurity ones. There are some apparent overlaps, but the disciplines have their peculiarities and, without passion, one cannot excel in any of them. So, in these years, we witnessed some programming talents fail miserably on CTF challenges, and, vice versa, some mediocre programmers excel in solving cybersecurity problems.

Cybersecurity is currently a hot topic, and young students are easily attracted and they *think* they love it, maybe thanks to videogames and TV series, but many of them give up when the technical part gets tough. Unfortunately, we do not have found a perfect recipe yet, and may only caution in trying to be too selective on the (a-posteriori) wrong skillsets.

We conclude this paper with a personal suggestion for those interested in following a similar experience. The project is exciting but - especially in the first year of adoption - it is also very demanding. The topic selection is rather broad, and it is tough for a single educator to cover all of them satisfactorily. Group collaboration is also needed from the teachers' perspective, and things become easier only in the following years if a community of young talents grows and helps the new entries, year after year. Without this help, it can become very frustrating and, honestly, pointless.

6 ACKNOWLEDGMENTS

The training activities would not have been possible without the cooperation of the ZenHack CTF team. We thank its members for their support and enthusiasm.

REFERENCES

[1] Dennis Andriesse, Xi Chen, Victor van der Veen, Asia Slowinska, and Herbert Bos. 2016. An In-Depth Analysis of Disassembly on Full-Scale x86/x64 Binaries. In *25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, Austin, TX, 583–600.

[2] S. Bratus. 2007. What Hackers Learn that the Rest of Us Don't: Notes on Hacker Curriculum. *IEEE Security Privacy* 5, 4 (July 2007), 72–75. https://doi.org/10.1109/MSP.2007.101

[3] Tom Chothia, Sam Holdcroft, Andreea-Ina Radu, and Richard J. Thomas. 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)*. USENIX Association, Vancouver, BC.

[4] C. Jämthagen, P. Lantz, and M. Hell. 2013. A new instruction overlapping technique for anti-disassembly and obfuscation of x86 binaries. In *2013 Workshop on Anti-malware Testing Research*. IEEE, Montreal, QC, Canada, 1–9.

[5] S. Maggiolo, G. Mascellani, and L. Wehrstedt. 2014. CMS: A growing grading system. In *Olympiads in Informatics*, Vol. 8. Vilnius University, 123–131.

[6] John R. Morelock and Zachary Peterson. 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)*. USENIX Association, Baltimore, MD.

[7] Patricia C. Salinas and Claudia Bagni. 2017. Gender Equality from a European Perspective: Myth and Reality. *Neuron* 96, 4 (2017), 721–729. https://doi.org/10.1016/j.neuron.2017.10.002

[8] Hovav Shacham. 2007. The Geometry of Innocent Flesh on the Bone: Return-into-Libc without Function Calls (on the X86). In *Proceedings of the 14th ACM Conference on Computer and Communications Security* (Alexandria, Virginia, USA) *(CCS '07)*. Association for Computing Machinery, New York, NY, USA, 552–561. https://doi.org/10.1145/1315245.1315313

[9] Laszlo Szekeres, Mathias Payer, Tao Wei, and Dawn Song. 2013. Eternal War in Memory. *IEEE Security & Privacy* 12, 48–62. https://doi.org/10.1109/SP.2013.13

[10] Valdemar Švábenský, Jan Vykopal, Milan Cermak, and Martin Laštovička. 2018. Enhancing Cybersecurity Skills by Creating Serious Games. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (Larnaca, Cyprus) *(ITiCSE 2018)*. Association for Computing Machinery, New York, NY, USA, 194–199. https://doi.org/10.1145/3197091.3197123

[11] Valdemar Švábenský, Jan Vykopal, and Pavel Čeleda. 2020. 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* (Portland, OR, USA) *(SIGCSE '20)*. Association for Computing Machinery, New York, USA, 2–8. https://doi.org/10.1145/3328778.3366816

[12] Muhammad Mudassar Yamin, Basel Katt, and Espen Torseth. 2020. Review of Training and Selection Processes for European Cyber Security Challenge 2019. Internal report.