A new adversarial training approach based on CTF

Andrea D'Urbano[1], Andrea Chezi[1] and Christian Catalano[1]

[1]CRLab, University of Salento, Italy

Abstract

Protecting digital assets has become a critical priority for individuals, businesses, and governments. As a result, there is a growing need for effective cybersecurity education that equips individuals with the skills and knowledge to identify, prevent, and respond to cyber threats. In this article, we examine the potential of using innovative educational methodologies, such as Capture the Flag (CTF), for teaching cybersecurity effectively and we propose an innovative educational methods. The platform to support it and an experiment to validate it are currently in progress.

Keywords

CTF, cybersecurity, education, training

1. Introduction

Cybersecurity is increasingly relevant, given that the cost of cybercrime is predicted to hit 8 trillion in 2023 and will grow to 10.5 trillion by 2025, according to the report [1]. With cybercrime and cyberthreats skyrocketing [2], is crucial to invest in prevention and education. Considering also the ever-changing nature of the complex field of cybersecurity, it is clear why traditional educational methods might not work as well as in other areas [3]. In this paper, we present a new approach to cybersecurity education based on Capture The Flag (CTF) challenges. Contrary to the traditional frontal lectures, these hands-on methods propose to complement theoretical knowledge with the creation of challenges related to the topics of interest, and in addition a competitive environment among groups of students that will exchange challenges. Furthermore, we are currently developing the platform to manage this new approach and an experiment testing the advantage of this new approach is about to start. We will begin by introducing the CTF world. We will then present the standard methodologies and compare them with our proposal, describing afterwards the platform itself. A brief comment on the experiment to test this new educational method is presented in the conclusion.

2. CTF: Capture the Flag

The term Capture the Flag (CTF) denotes a typology of cybersecurity competition that challenges participants to find and exploit vulnerabilities in a (simulated or, more rarely, real) computer system or network. These competitions can be designed to mimic real-world cybersecurity

IS-EUD 2023: 9th International Symposium on End-User Development, 6-8 June 2023, Cagliari, Italy

andrea.durbano@unisalento.it (A. D'Urbano); andrea.chezi@unisalento.it (A. Chezi); christian.catalano@unisalento.it (C. Catalano)

scenarios or, from a different perspective, they can be viewed as cyber-puzzles, often containing a recurrent story or theme deeply rooted in the underground culture. The ultimate objective of these challenges is to capture the flag by finding all the hidden information before other participants. CTF competitions are often used for education and training, as well as to evaluate and improve the security of real-world systems.

In CTF competitions, participants must retrieve the so-called "flag", a particular string of text hidden in files or sensitive information that can only be accessed through exploiting some vulnerabilities in the system. It is common to find multiple ways to solve a specific challenge. Even more, it is possible that 0-days vulnerabilities (i.e., not previously known vulnerabilities) are found during CTF competitions (see for example [4, 5]).

CTF competitions are an excellent tool for cybersecurity education and training [6, 7] since they provide a safe and controlled environment for participants to gain hands-on experience in identifying and exploiting vulnerabilities, which is essential for developing practical cybersecurity skills. Furthermore, they can be used to identify potential vulnerabilities in real-world computer systems and networks, allowing organizations to patch them before malicious actors can exploit them. The competitions can range from local events held at universities or hackathons to international competitions with large cash prizes. One example is DEF CON CTF [8], a yearly competition in Las Vegas during the world's most famous cybersecurity conference. Other famous examples are Google CTF, Codegate CTF, held annually in South Korea, Pwn2Own, where participants need to find 0-days vulnerabilities and held bi-annually at the CanSecWest security conference. Many of these competitions involve prize pools of several thousand dollars. To be updated on CTF events as well as ranking of competitions and teams around the worlds, the reference website is "CTFtime" [9].

CTF competitions can be categorized into various classes: Jeopardy, Attack-and-Defense (A/D), King of the Hill (KotH), Boot2Root and mixed style. A Jeopardy CTF is a series of challenges, of increasing difficulty (and hand in hand worth increasing scores), divided into categories such as web, binary exploitation, cryptography etc...
Upon expiration of the given time, the participants with the highest score win.

In the category A/D, each team is given a server with a certain number of vulnerable services, used periodically by a bot. This bot generates and writes flags on each server. Participants are expected to patch the vulnerabilities on their services, while keeping them working (Defend) and exploit the same vulnerabilities on the other teams (Attack). The final score is computed by counting how many flags each team has stolen, and other parameters to evaluate the goodness of defence. In King of the Hill category, teams compete to gain control of a vulnerable system or network and maintain control for as long as possible. The team that maintains control for the longest time wins. In boot2root CTFs, teams are presented with vulnerable virtual machines. The goal is to gain admin privileges. In the mixed category, all the other type of CTF competitions are considered. Some examples are competitions where all the challenges are obtained from real used applications; as already mentioned, there can be competitions with the objective of finding 0-days. Other CTFs can involve physical devices, such as smart cars or satellites.

3. Proposed methodology

Teaching cybersecurity can be challenging, given that the field is in constant and fast pacing evolution. Relevant aspects must also be taken into account, such as the time and the resources available to the educators, as well as the target audience. Since the environment and the challenges contended by a cybersecurity expert change continuously, it can be said that actually the learning process never ends. The traditional teaching method of cybersecurity, at all levels, usually involve a lecture-based approach. Lectures on selected topics in cybersecurity are delivered to the students, depending on the specific goals and the time available to reach them. The program covered in a month by a group of student already working in IT, with experience in digital security assessment, will be necessary different from the one covered by a group of high school students in a semester preparing to compete in a CTF. This lecture based approach can be useful to teach theoretical concepts, but can be lacking in building specific skills required by the specific goals: for example writing a cybersecurity report after a penetration test for a company or solving binary exploitation challenges involving a 0-day. Some skills cannot simply be teached, they must be acquired through experience. For this reason other hand-on approaches are taken into account when programming an educational intervention. This approaches focuses on practical exercises where students can gain experience with the security tools and techniques they will use in the actual job they should be prepared for. Simulations, laboratories and scenario-based training can all be valid hands-on approaches. As an useful complement, individual or group cybersecurity projects can be assigned in order to give the necessary time to understand the problems and the solutions involved in the specific project. Some example projects can include tasks such as creating a security policy, conducting a vulnerability assessment, and designing a secure network. Using CTF for cybersecurity education can be a clever move since it takes advantage of the gamification of the learning process [10]. Learning cybersecurity through CTF competitions could improve engagement from students and, therefore, the overall learning process [11]. Nevertheless using CTF challenges as a means to introduce or advance in cybersecurity has the disadvantage of not being flexible enough to allow for its use on a wide range of participants. Actually, challenges are often far from real-world cases, or wildly varying in difficulty of solution. For these reasons, we present a new teaching model for learning cybersecurity, where groups of students challenge each other by creating CTF problems. Students would be divided into groups of approximately the same size, then each group should collaborate to create challenges on selected topics, strictly related to the learning objectives specific to each course. The challenges should then be proposed to all other groups or just to a subset of them, giving in this way control on the targeting of topics and student groups. Using this new learning methodology we expect a greater engagement from the students, possibly resulting in better results on the final score.

4. Platform design

In order to support the adoption of this new method, we are developing a platform to help us in the endeavour. It is worth noting that online there is a moltitude of resources on CTF training, as well as cheatsheets, code snippets and learning platforms. Some famous examples

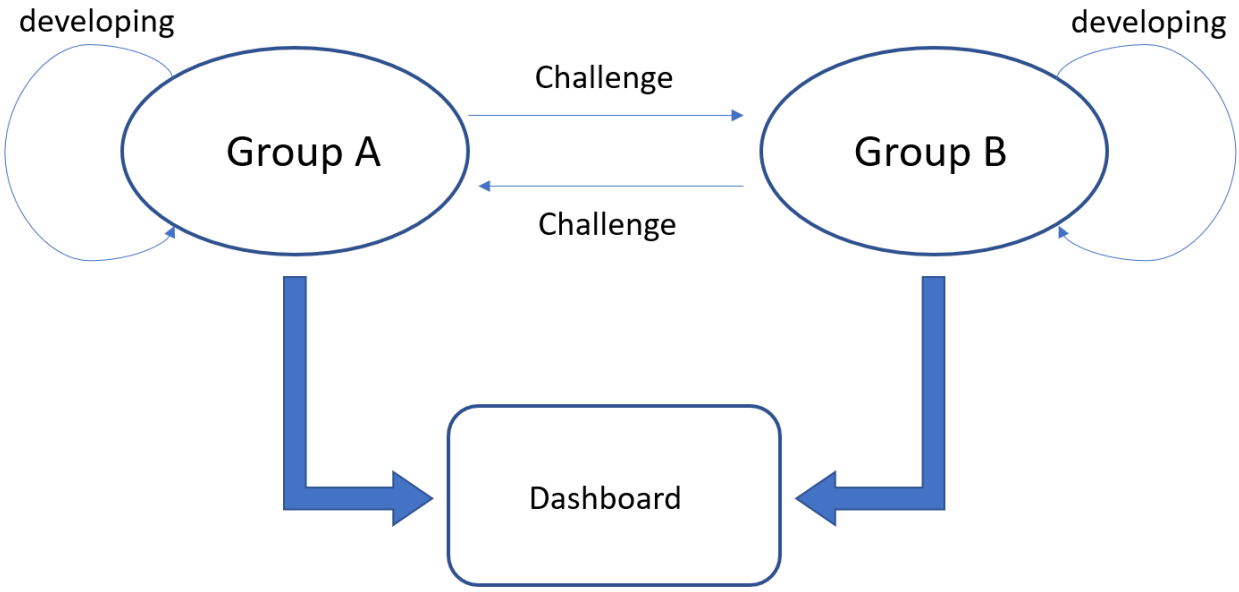

Figure 1: Example scheme with two groups. Both groups in the developing phase, create new CTF challenges. The teams then challenge each others and the results are displayed on the scoreboard.

include but are certainly not limited to ”TryHackMe” [12] and ”HackTheBox” [13] where both free and subscription plan exists. Both platforms present cybersecurity topics as a series of lectures and related challenges. There exist also category specific platforms, such as for example ”exploit.education” and ”pwn.college” for binary exploitation category and ”cryptohack” for crypto. The platform currently under development (sketched in figure 1) will have the same base structure of a standard CTF platform: an homepage containing some general rules and guidelines; the scoreboard where the current ranking of participants is shown, as well as who solved which challenge; the challenges divided by category and ordered by points or time of release. In addition, each team will have a personal space where it will possible to upload the challenges created and where the teams to be challenged will be selected. Finally, a ”story mode” will be present, allowing each participant to experience a story and solve mysteries using cybersecurity skills acquired by playing.

5. Future Work and Conclusion

From the 21st of April 2023, the platform as well as the new learning methodology will be tested at Department of Computer Science, University of Bari. Students will be divided in a control group, and an experimental group. Every student was preliminarly tested on knowledge and competencies in cybersecurity: the knowledge, using a quiz, while the competencies using 4 simple CTF challenges to be solved in a given time. Successively, for the time of the experiment (i.e. until the end of the course), the two groups will be subjected to different teaching methodologies. The control group will attend regular frontal lectures while the experimental group will use the platform to create and share CTF challenges on the studied topics. At the end of the course, students will be tested again on knowledge and competencies. We expect to

see an increase in the competencies in the experimental group and an equal level of knowledge. The acquired evidence will be the basis for appropriate statistical tests to accept or refuse the previous assumption.

This innovative methodology, as well as the proposed platform, can be applied to various contexts, ranging from introductory-level cybersecurity education to university-level courses and professional-level updating courses in the industry. Future work will foster the integration of the present proposal with other architectures for knowledge transfer in the cybersecurity domain [14] and with current methodological and technological frameworks for learning [15, 16].

Acknowledgments

Andrea Chezzi and Andrea D'Urbano acknowledge the funding received by Deep Consulting S.r.l. within the framework Ph.D. program in Engineering of Complex Systems.

References

[1] Esentire, 2022 official cybercrime report, https://www.esentire.com/resources/library/2022-official-cybercrime-report, 2022.
[2] P. I. IBM, Cost of a data breach 2022, https://www.ibm.com/reports/data-breach, 2022.
[3] A. McGettrick, Toward effective cybersecurity education, IEEE Security & Privacy 11 (2013) 66–68.
[4] Wallarm, Php remote code execution 0-day discovered in real world ctf exercise, https://lab.wallarm.com/php-remote-code-execution-0-day-discovered-in-real-world-ctf-exercise/, 2019.
[5] NIST, Php remote code execution 0-day discovered in real world ctf exercise, https://nvd.nist.gov/vuln/detail/CVE-2022-4349, 2022.
[6] E. Trickel, F. Disperati, E. Gustafson, F. Kalantari, M. Mabey, N. Tiwari, Y. Safaei, A. Doupé, G. Vigna, Shell we play a game? ctf-as-a-service for security education., in: ASE@ USENIX Security Symposium, 2017.
[7] A. Mansurov, et al., A ctf-based approach in information security education: an extracurricular activity in teaching students at altai state university, russia, Modern Applied Science 10 (2016) 159.
[8] C. Cowan, S. Arnold, S. Beattie, C. Wright, J. Viega, Defcon capture the flag: Defending vulnerable code from intense attack, in: Proceedings DARPA Information Survivability Conference and Exposition, volume 1, IEEE, 2003, pp. 120–129.
[9] Ctftime, https://ctftime.org/, 2023.
[10] G. Kiryakova, N. Angelova, L. Yordanova, Gamification in education, in: Proceedings of 9th international Balkan education and science conference, volume 1, 2014, pp. 679–684.
[11] K. Boopathi, S. Sreejith, A. Bithin, Learning cyber security through gamification, Indian Journal of Science and Technology 8 (2015) 642–649.
[12] Tryhackme, https://tryhackme.com/, 2023.
[13] Hackthebox, https://www.hackthebox.com/, 2023.

[14] C. Catalano, P. Afrune, M. Angelelli, G. Maglio, F. Striani, F. Tommasi, Security testing reuse enhancing active cyber defence in public administration., in: ITASEC, 2021, pp. 120–132.
[15] M. T. Baldassarre, V. Santa Barletta, D. Caivano, D. Raguseo, M. Scalera, Teaching cyber security: The hack-space integrated model., in: ITASEC, 2019.
[16] V. S. Barletta, F. Cassano, A. Marengo, A. Pagano, J. Pange, A. Piccinno, Switching learning methods during the pandemic: A quasi-experimental study on a master course, Applied Sciences 12 (2022) 8438.