Introducing Penetration Test with Case Study and Course Project in Cybersecurity Education

Xinli Wang
School of Computing
Grand Valley State University
Allendale, Michigan, USA
wangx@gvsu.edu

Yan Bai
School of Engineering and Technology
University of Washington Tacoma
Tacoma, Washington, USA
yanb@uw.edu

Abstract—Teaching college students ethical hacking skills is considered a necessary component of a computer security curriculum and an effective method for teaching defensive techniques. However, there is a shortage of textbooks and technical papers that describe the teaching materials and implementation of penetration testing techniques for hands-on exercises. In our teaching practice, we have been using case studies and course projects as a means to help students learn the fundamental concepts of, primary techniques and commonly used tools for penetration testing. We think this is a beneficiary complement of a cybersecurity course that is taught in a defensive approach. Through these activities, students have gained hands-on experience and developed their ethical hacking skills. Feedback from them is positive and student learning outcomes are promising. In this paper, we describe the principles of developing and implementing case studies and course projects along with associated considerations for specified educational objectives when introducing penetration test. An example case study and course project that we have been using in our courses are described to introduce the major design ideas and activities to complete them. Experience, lessons and the feedback from students are discussed. Our results will provide a good point of reference for those educators who teach a cybersecurity course at a college or university and would like to offer an introduction to ethical hacking. This work can also be a reference for a college that wants to integrate penetration testing into its cybersecurity curriculum.

Keywords—ethical hacking, penetration testing, security education, course project, case study

I. INTRODUCTION

Nowadays, ethical hacking (EH), or penetration testing (PT), has become an integral component of information technology (IT) management for industry compliance, security hygiene and proactive defense [1]–[4]. To meet the growing demand for EH professionals from the IT industry, researchers and educators agree that teaching PT and adversarial thinking at a university is a necessary component of a cybersecurity curriculum [5]–[7]. Ethical hacking and adversarial thinking are recommended as an important component in a cybersecurity curriculum by the joint task group on information technology curricula [8] and cybersecurity education [9]. In practice, however, as argued by Trabelsi *et al.* [7], it is burdensome to teach students to hack ethically at a university due to the shortage of hands-on exercise implementation.

In our teaching practice, we have employed the following two approaches to introducing the basic concepts and skills of PT in a cybersecurity course that is taught in a defensive way:

- **Case Study**: A system with vulnerabilities is implemented and configured by the instructor and provided to the students. With a case description of the system and minimal hints, students are allowed to explore and hack into this system.
- **Course Project**: Students are grouped up. Each group will create a system with vulnerabilities first. Then, this system is exposed to another group to allow them to explore and hack into it. A description of the system will be provided along with minimal hints.

For simplicity, however, we will generally call both types of hands-on activities as "project" below.

Students' feedback is positive. These hands-on activities have inspired student's interest in cybersecurity. In this paper, we will explain the principles and considerations of project design. An example case study and a course project will be described to illustrate their implementations. We will also share our experiences and lessons that have been learned from our teaching practice. Results of this paper will be helpful to those who are teaching or going to teach a cybersecurity course and would like to introduce the concepts and skills of ethical hacking. Our experiences and lessons can also serve as a point of reference for the curriculum development in cybersecurity.

II. RELATED WORK

Researchers have suggested different approaches to expose specific aspects of EH to college students. Examples include a penetration testing box [10], red-team experience [11] and online courses [12]. Trabelsi and Ibrahim [13] describe the implementation of a case study to make three classic denial-of-service attacks for teaching EH. Wu [14] offers a course project for EH in a website security course. Dimkov *et al.* [15]–[17] present an interesting practical assignment in computer security education that integrates physical security, social engineering attack and digital penetration testing. More recently, a Raspberry Pi-based lab architecture is used for teaching EH skills [18]. Wang *et al.* [19] propose an undergraduate course curriculum for EH. Yue and Park [20] propose a set of virtual labs for an EH course based on Kali Linux [21]. Cyber Range platforms have been commonly employed to teach EH [22], [23] and the learning outcomes are promising.

III. Project Design and Implementation

We consider the following aspects when designing the course project and case study for introducing EH skills and approaches:

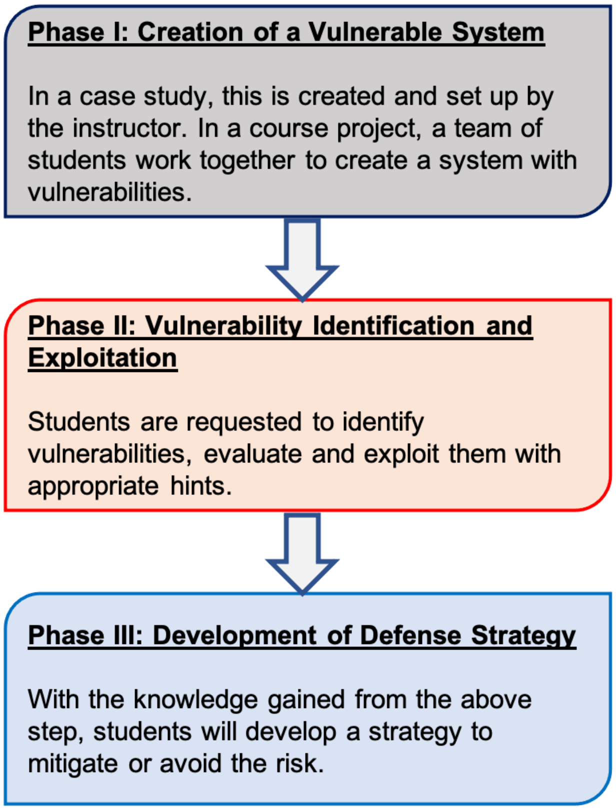
- **Fun *vs.* knowledge**: Making a project fun will always attract more interest from students and receive a higher student evaluation score. However, as a component of course curriculum, we need to have clear educational objectives and expected learning outcomes. We want to embed knowledge gaining in fun activities.
- **Legal and ethical issues**: A legal statement is always included in an assignment to inform students that hacking itself is illegal. An example legal statement is given below:

> *"We hack for learning, not learn for hacking. You are not allowed to use the techniques gained from this course for any malicious purpose. Any malicious action is illegal and will be caught and prosecuted."*

In order to help students develop the mindsets and skills for EH, a project is designed with the following general educational objectives:

- Motivate students to use the techniques and software tools learned in class to identify vulnerabilities and exploit them.
- Help students gain analytical and problem-solving skills and the mindsets that are essential for PT by exploring, examining and analyzing provided cases.
- Inspire the spirit of team work, self-learning, experience and knowledge sharing, and active learning.

To achieve the above educational objectives, a course project is designed as a three-phase work. A framework is shown in Fig. 1. A case study can be completed either individually or in a team. We highly encourage completing a course project in a team. Student groups are organized based on mutual agreement. Ideally, each team consists of 4-5 students from different backgrounds (*e.g.*, computer science, information systems, IT, *etc.*) to promote knowledge and experience sharing.



Phase I: Creation of a Vulnerable System

In a case study, this is created and set up by the instructor. In a course project, a team of students work together to create a system with vulnerabilities.

Phase II: Vulnerability Identification and Exploitation

Students are requested to identify vulnerabilities, evaluate and exploit them with appropriate hints.

Phase III: Development of Defense Strategy

With the knowledge gained from the above step, students will develop a strategy to mitigate or avoid the risk.

Fig. 1. A framework for project design

The first step is the provision of a system that has vulnerabilities on purpose. For a case study, the course instructor will develop and set up such an environment and expose it to the students with minimal hints. In a course project, such a system is developed and configured by a team of students.

When a vulnerable system has been provided, students will try to unearth the vulnerabilities and exploit them in the second phase. Students are encouraged to apply the knowledge and use the tools learned from this course or obtained from their own experience to diagnose and pinpoint the vulnerabilities. Then, they will try to exploit the identified weakness to gain access to the system or make attacks to the application.

The major purpose of the third phase is to evaluate the learning outcomes of the project since the goal of PT is to develop a defense plan. This strategy can be proposed by the students themselves or through a follow-up class discussion. In our teaching practice, the defense strategy will be developed by the students in a course project and presented in class. Usually, the proposed strategy will be improved in response to audience input during a Q&A section. For a case study, the defense strategy is included in the case study report and discussed in class since all of the students have been exposed to the same vulnerabilities.

IV. Example Project and Case Study

An example case study and course project that have been used in our courses are presented in this section[1]. Case and project descriptions are modified to hide personal or sensitive information.

A. A Treasure Hunt Case

This case study is given right after Nmap network scanner [24] and Hydra online password cracker [25], [26], that come with Kali Linux [21], have been introduced in a previous lab in a senior level undergraduate cybersecurity course at a four-year college. Students can be from different backgrounds, including computer science, IT, cybersecurity and information system.

1) Case Description: The network design for this case study is depicted in Fig. 2. The instructor sets up an SSH server on one virtual machine (VM) and it is connected to the Local Area Network (LAN, a virtual network). A number of user accounts are created for remote access to this server.

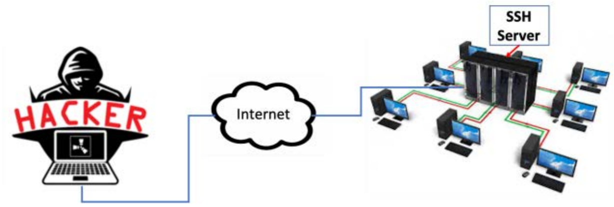


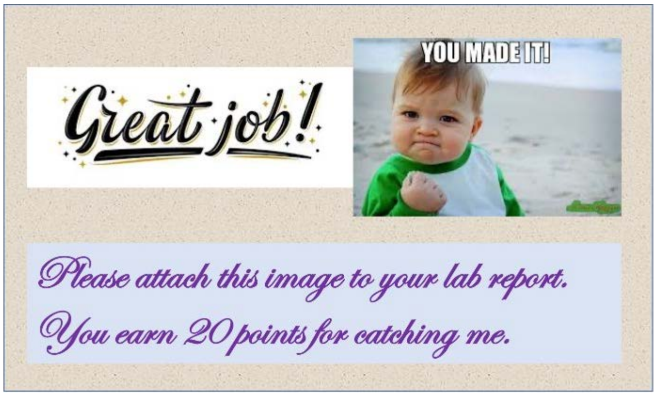
Fig. 2. Network design diagram for an example case study

One of the user accounts is created with a known user name (the name of the course, which is easily predictable) and a password that is from the Rockyou word list [27]. This user account simulates the credentials of the grader for this course. Two valuable files are created and hidden under the home directory of this user along with many other files that are not relevant. On each of these two files, the points that a student can receive when he or she manages to steal it are specified.

The case description reads as follows:

> You have recently heard that the grader of this course stores grading files on a VM on our network. For curiosity, you want to gain access to his account and find the grading sheet. To facilitate your adventure, I have collected the following basic information for you:
>
> - The grader’s account is on one of the following servers:
>
>   - IP 1
>
>   - IP 2
>
>   ... ...
>
>   - IP n
>
> - The username of the grader: ***cs456***.
>
> - To start with, a good Wordlist, such as Rockyou Wordlist, can be used to crack a password.
>
> - You don’t have physical access to the server because it is physically locked in a secured room

2) Vulnerability Identification and Exploitation: When this case study is assigned and the vulnerable system is exposed to the students, most of them start by conducting a port scan with Nmap [24] against the given IP addresses in the list. They find two SSH servers. Then, they try to crack the grader’s password online with Hydra. Then, they log in to this server with the discovered password. After gaining access to the server, most of the students find the two valuable files in 2-3 hours. One of them is shown in Fig. 3.



Please attach this image to your lab report.
You earn 20 points for catching me.

Fig. 3. An example valuable file for case study

This case study can be completed individually or in a group. Each group or individual is required to submit a report to explain what they did to find those two files and how they would have hardened this server to mitigate the risk of being hacked. From the report, we can see that students have been actively engaged in this activity by asking questions, sharing experiences, and conducting independent research. Most of them have done more than required. For example, some students use different network scanners, including Nmap [24] and Metasploit [28], to scan the IP addresses in the given list and compare their differences. Some attempt gSOAP attacks from the list of exploits [29]. A number of them use the **find** utility to search for interesting files. Others describe a very good defense plan and share their working experiences.

3) Development of Defense Strategy: As expected, we have achieved the student learning outcomes by working out a defense strategy in a follow-up class discussion. Here are some suggestions from our students:

- I would scan my network periodically and close unnecessary open ports.

[1] **Disclaimer**: *Names and organizations used in these examples are for presentation purpose only. They are not real. The authors are not responsible for any legal issues if there is any coincidence*

- I would implement a user logout mechanism to lock out the system after three unsuccessful login attempts.
- For important accounts, I would perform proactive password cracking to ensure that all passwords are strong and not listed on a known word list.
- I would locate important servers on a network that is specifically hardened with a firewall that does not allow outbound traffic except that to specific servers.
- I would set up multi-factor authentication for critical user accounts.

We think this is a very good strategy to defend against the vulnerabilities exposed in this case study. Student feedback is positive as quoted below:

> *"That was a really enjoyable and rewarding project. I won't forget how important a strong password is in reality. The techniques and the adversarial thinking would be helpful in my whole life."*

B. *A Self-Motivated Course Project*

We have designed a course project in a senior undergraduate computer security course for students to evaluate the security of a Linux system and identify the points of exploitation. Then, they apply various security mechanisms, such as access control, file protection and authentication, to secure the system. The project is designed for group work. As depicted in Fig. 1, it mainly consists of three phases. In the first phase, each team will produce a vulnerable virtual Linux system for later exploitation by another team and record the vulnerabilities that they have produced. To make it challenging, each team is required to produce a total of 32 pieces of vulnerabilities in eight different areas (reference Jang and Messier [30] for details), including invoking and running a process, user privileges and permissions, file system, encryption, services, network and firewall, applications, alerts and updates. In the second phase, each group will investigate another team's vulnerable system created in Phase I. Finally, they remove the vulnerabilities, harden the Linux system, and submit a project report that describes what they have done and how to ensure the security of a Linux system. Throughout the three phases, students learned both offensive and defensive knowledge and skills. Students were very engaged throughout their project work. Their final project reports have demonstrated that they are able to integrate what they have learned from the class, such as Linux information security policies and procedures, and Linux system protection and controls, to provide an effective security improvement solution for a vulnerable system.

Table I shows an example set of vulnerabilities in eight different areas created by our students in Project Phase 1 that are covered in Jang and Messier [30]. These vulnerabilities are linked to different risk levels: high, medium, and low. Students from a peer team were able to successfully identify and fix those vulnerabilities by using appropriate commands and editing relevant configuration files in a Linux system.

TABLE I. EXAMPLES OF PLANNED VULNERABILITIES IN PROJECT PHASE 1

Area	**Vulnerability Created**	**Risk Level**
Getting Up and Running	Unnecessary sudo access	High
	Grub without password-protection	High
User Privileges & Permissions	Weak password aging control	Medium
	No account lockout	High
File Systems	Writable and executable boot	High
	A file containing root password	High
Encryption	Unencrypted private file	High
	Old version of SSL	Medium
Service	Telnet enabled	Low
	Disabled SELinux	Medium
Network and Firewalls	IPtables not configured correctly	Medium
	Constantly running Apache	Medium
Application	Unsecure NTP server	Medium
	Open ports for unneeded services	Low
Alerts and Updates	No alerts to user for downloading available updates	Medium
	Disabled auto system updates	Low

Feedback from students is positive as quoted below:

> *"This project was very hands-on and an informative experience. I believe this [will] be very beneficial in the field. On a large scale, finding common default vulnerabilities would be a key to the success of the company. Once discovering the steps to remediate the vulnerabilities, a script can be made to automate the process to expedite the remediation for future devices. Linux commands will [be] around for a long time, especially with the open-source usability individuals have full leisure of at their fingertips."*

V. Conclusion

We consider the case study and course project as a good option for exposing college students to the fundamental principles and primary skills of EH in a cybersecurity course that is taught with a defensive approach. In order to achieve educational objectives and student learning outcomes, both the case study and course project need to be well designed to balance enjoyment and knowledge acquisition. Legal and ethical concerns must also be handled seriously according to the IT policy of a university. We have presented the considerations and guidelines that we follow in our teaching practice when designing and implementing a case study and course project along with general educational objectives. These principles have been illustrated in the example case study and course project. As PT and adversarial thinking are a necessary component in a security curriculum or a cybersecurity program [5]–[9], [13], [31]–[34], our results can serve as a strong reference for those who are teaching or will teach a cybersecurity course with a defensive approach at a college or university. The materials from the example case study and course project can be used by an educator with minimum modification to better fit to their specific networks and IT policies.

To develop a more comprehensive course project to reflect real-world observations, we will guide students to create system vulnerabilities according to a standard classification, such as the MITRE ATT&CK© [35] in the future.

Acknowledgement

This research was, in part, supported by National Science Foundation (NSF) Grant 1921576.

References

[1] D. Bonilla, “Ethical hacking emerges as unique career path in cybersecurity,” tech.co, April 27 2017, https://tech.co/news/ethical-hacking-career-cybersecurity-2017-04. Last visited on May 16, 2021.

[2] Hackerone, “Rethink your traditional pentests,” Online, June 11 2020, https://www.hackerone.com/resources/e-book/rethink-your-traditional-pentests. Last retrieved on May 26, 2021.

[3] Paul, “Ethical hacking career: A career guideline for ethical hacker,” edureka, Online, November 25 2020, https://www.edureka.co/blog/ethical-hacking-career/. Last visited on May 16, 2021.

[4] Coursera, “5 cybersecurity career paths (and how to get started),” Online, September 20 2021, https://www.coursera.org/articles/cybersecurity-career-paths. Last visited on December 31, 2021.

[5] S. Bratus, “Hacker curriculum: How hackers learn networking,” *IEEE Distributed Systems Online*, vol. 8, no. 10, pp. 2–2, 2007.

[6] V. Subhashini, “Ethical hacking and legal systems,” *Internal Journal of Emerging Technology in Computer & Electronics (IJETCSE)*, vol. 11, no. 4, pp. 36 – 40, 2014.

[7] Z. Trabelsi and M. McCoey, “Ethical hacking in information security curricula,” *Int. J. Inf. Commun. Technol. Educ.*, vol. 12, no. 1, p. 1–10, Jan. 2016. [Online]. Available: https://doi.org/10.4018/IJICTE.2016010101

[8] Task Group on Information Technology Curricula, “Information technology curricula 2017 final report,” online, December 10 2017, https://www.acm.org/binaries/content/assets/education/curricula-recommendations/it2017.pdf. Last retrieved on May 12, 2021.

[9] Joint Task on Cybersecurity Education, “Cybersecurity curricula 2017 – curriculum guidelines for post-secondary degree programs in cybersecurity,” online, December 31 2017, https://www.acm.org/binaries/content/assets/press-releases/2018/february/cybersecurity-curricula-17.pdf. Last retrieved on May 12, 2021.

[10] L. Epling, B. Hinkel, and Y. Hu, “Penetration testing in a box,” in *Proceedings of the 2015 Information Security Curriculum Development Conference*. New York, NY, USA: Association for Computing Machinery, 2015, pp. 1–4. [Online]. Available: https://doi.org/10.1145/2885990.2885996

[11] S. Cunha, W. Winders, D. C. Rowe, and C. Cornel, “The untrustables: How underclassmen evolved our approach to student red-teaming,” in *Proceedings of the 17th Annual Conference on Information Technology Education*. New York, NY, USA: Association for Computing Machinery, 2016, pp. 26–30. [Online]. Available: https://doi.org/10.1145/2978192.2978213

[12] T. N. Nguyen, “Certified ethical hacker v. 10 online course: a case study,” in *Proceedings of the 10th International Conference on E-Education, E-Business, E-Management and E-Learning*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 168–173. [Online]. Available: https://doi.org/10.1145/3306500.3306547

[13] Z. Trabelsi and W. Ibrahim, “Teaching ethical hacking in information security curriculum: A case study,” in 2013 *IEEE Global Engineering Education Conference (EDUCON)*. New York, NY, USA: IEEE, March 2013, pp. 130–137.

[14] A. J. Wu, “Project development for ethical hacking practice in a website security course,” in *Proceedings of the Western Canadian Conference on Computing Education*, ser. WCCCE ’14. New York, NY, USA: Association for Computing Machinery, 2014. [Online]. Available: https://doi.org/10.1145/2597959.2597963

[15] T. Dimkov, A. van Cleeff, W. Pieters, and P. Hartel, “Two methodologies for physical penetration testing using social engineering,” in *Proceedings of the 26th Annual Computer Security Applications Conference*, ser. ACSAC ’10. New York, NY, USA: Association for Computing Machinery, 2010, p. 399–408. [Online]. Available: https://doi.org/10.1145/1920261.1920319

[16] T. Dimkov, W. Pieters, and P. Hartel, “Effectiveness of physical, social and digital mechanisms against laptop theft in open organizations,” in *Proceedings of the 2010 IEEE/ACM International Conference on Green Computing and Communications & International Conference on Cyber, Physical and Social Computing*, ser. GREENCOM-CPSCOM ’10. USA: IEEE Computer Society, 2010, p. 727–732.

[17] T. Dimkov, W. Pieters, and P. Hartel, “Training students to steal: A practical assignment in computer security education,” in *Proceedings of the 42nd ACM Technical Symposium on Computer Science Education*, ser. SIGCSE ’11. New York, NY, USA: Association for Computing Machinery, 2011, p.21–26. [Online]. Available: https://doi.org/10.1145/1953163.1953175

[18] P. James, L. Powell, L. O’Reilly, and F. Moller, “Hands-on security testing in a university lab environment,” in *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education*, ser. ITiCSE ’20. New York, NY, USA: Association for Computing Machinery, 2020, p. 68–74. [Online]. Available: https://doi.org/10.1145/3341525.3387366

[19] Y. Wang, M. McCoey, and Q. Hu, “Developing an undergraduate course curriculum for ethical hacking,” in *Proceedings of the 21st Annual Conference on Information Technology Education*, ser. SIGITE ’20. New York, NY, USA: Association for Computing Machinery, 2020, p. 330–335. [Online]. Available: https://doi.org/10.1145/3368308.3415366

[20] X. Yue and H. Park, “Design of virtual labs for an ethical hacking course,” *J. Comput. Sci. Coll.*, vol. 35, no. 6, p. 31–38, Apr. 2020.

[21] Kali, “Kali Linux web site,” online, https://kali.org/. Last visited on May 16, 2021.

[22] G. Di Tizio, F. Massacci, L. Allodi, S. Dashevskyi, and J. Mirkovic, “An experimental approach for estimating cyber risk: a proposal building upon cyber ranges and capture the flags,” in *2020 IEEE*

European Symposium on Security and Privacy Workshops (EuroS PW), 2020, pp. 56–65

[23] Cyberbit, “Cyber bit home page,” Online, 2020, https://go.cyberbit.com/cyber_security_training-platform/. Last visited on June 6, 2021.

[24] NMAP.ORG, “Nmap web site,” online, https://nmap.org/. Last visited on May 16, 2021.

[25] Hydra Team, “Hydra home page,” Online, https://github.com/vanhauser-thc/thc-hydra. Last visited on November 12, 2021.

[26] Kali Team, “Hydra usage example,” Online, https://www.kali.org/tools/hydra/. Last visited on November 12, 2021.

[27] V. Kumar, “Rockyou wordlist kali location and uses, complete tutorial for beginners,” Online, March 11 2021, https://www.cyberpratibha.com/blog/how-do-i-use-rockyou-wordlist-txt-in-kali-linux/. Last retrieved on June 1, 2021.

[28] Metasploit, “Home page,” Online, May 28 2021, https://www.metasploit.com/. Last retrieved on June 1, 2021.

[29] Metasploit Database, “gSOAP 2.8 - directory traversal,” Online, November 13 2019, https://www.exploit-db.com/exploits/47653. Last retrieved on June 1, 2021.

[30] M. Jang and R. Messier, *Security Strategies in Linux Platforms and Applications*, 2nd ed. 5 Wall Street, Burlington, MA, USA: Jones & Bartlett Learning, October 20 2015.

[31] S. Bratus, “What hackers learn that the rest of us don’t: Notes on hacker curriculum,” *IEEE Security & Privacy*, vol. 5, no. 4, pp. 72–75, 2007.

[32] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, Jøsang, T. Pereira, and E. Stavrou, “Global perspectives on cybersecurity education for 2030: A case for a meta-discipline,” in *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, ser. ITiCSE 2018 Companion. New York, NY, USA: Association for Computing Machinery, 2018, p. 36–54. [Online]. Available: https://doi.org/10.1145/3293881.3295778

[33] V. Svabensky, J. Vykopal, and P. Celeda, “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*, ser. SIGCSE ’20. New York, NY, USA: Association for Computing Machinery, 2020, p. 2–8.

[34] A. Ahmed, K. Lundqvist, C. Watterson, and N. Baghaei, “Teaching cyber-security for distance learners: A reflective study,” in *2020 IEEE Frontiers in Education Conference (FIE)*, 2020, pp. 1–7.

[35] MITRE ATT&CK, “ATT&CK home page,” Online, 2021, https://attack.mitre.org/. Last visited on November 12, 2021.