Cybersecurity education is a relatively new topic in most educational organizations today. This poses a problem to most educational institutions like universities, which confront the challenge of teaching cybersecurity to students that do not have the necessary skills and knowledge to understand these topics. Across the United States and other countries, different initiatives have emerged to deal with this problem [2, 3]. They range from creating all the needed resources in the university to directing the student to resources outside the university.

This project is intended to deal with the problem by creating labs that teach the students skills and topics in cybersecurity, like the ones presented in the National Cyber League (NCL) competition, and later use the NCL platform as a testing ground. The main benefit of our approach is being able to fill those skill and knowledge gaps students have by tailoring each lab using the NCL competition as a reference.

Introduction

The purpose of this project was to develop the labs for a cybersecurity introductory course. These were created inspired by the NCL Challenges and the topics that are introduced in this competition through its different parts. NCL is a Jeopardy-type Capture The Flag (CTF), which mainly purpose is to serve as an educational tool to introduce people to cybersecurity and their continued development in cybersecurity [1].

The idea of this project emerges from a proposal for my master project given by my mentor Dr. Jeffrey Duffany, which consists in creating tutorials that serve as guide for students to learn about cybersecurity concepts and tools, skills that are key in the NCL competition and other CTF competitions.

This is something that was seen before in a Penetration Testing course given by two student peers, Yoshuah Alichea and Steven Bonnet. In this course, different cybersecurity concepts and different tools were taught to the students, first by introducing the cybersecurity concept or tool and later, by solving a Capture The Flag (CTF) challenge. This way of teaching cybersecurity increases student engagement and leads to more well-developed skills [1, 4].

Problem

I aim to create an educational package to teach about cybersecurity within my educational institution. My goal is to create labs that teach the students about cybersecurity by taking in consideration the knowledge and skills of the students [5], at the same time they engage in cybersecurity competitions that will enable them to keep developing their skills and gaining more knowledge all year round. Identify what resources are necessary for the students to achieve the goals mentioned above that doesn’t require a major investment from the university.

Conclusion

The work described throughout this project will serve to improve the content of the Penetration Testing Course by providing written content, practical exercises and tools for the students in a convenient and accessible way. It could also be used as material for other courses related to cybersecurity or that at least covers one of the topics of the labs. It will provide the students with the necessary knowledge and skills to compete in the NCL competition and other CTF competitions, so these can continue reinforcing their skills and gaining more knowledge.

Future Work

The labs need to be tested on a group of students who later on will compete in the NCL competition and preferably have not competed before in NCL, so they can provide a better feedback about how the labs actually helped them gain those skills and knowledge, and how easy to follow they were. Depending on the evaluation by the students and professor and the results of the NCL competition, the labs should be evaluated in order to decide whether they need changes or not.

Also, it is necessary to continue the process of generating exercises that later on can be integrated into other ongoing cybersecurity educational projects that make use of the labs and exercises.

Acknowledgements

I want to thank my mentor professor, Dr. Jeffrey Duffany, for all his support throughout this project. Also, I want to thank Yoshuah Alichea and Steven Bonnet for helping me with the Penetration Testing course, which serve as a reference point for this project.

This material is based upon work supported by, or in part by the National Science Foundation Scholarship for Service (NSF-SFS) award under contract/award # 1563797.

References