National Cyber League Challenges As A Way To Teach Cybersecurity

Author: André Agosto Quiñones
Advisor: Dr. Jeffrey Duffany
Electrical & Computer Engineering and Computer Science Department

Abstract

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 can 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 main 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, Yoshuam Alicea and Steven Bennet. 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.

Methodology

I began asking myself three questions: What am I trying to teach? Who am I trying to teach? What is the end purpose of this educational activity? I knew what topics needed to be covered because the NCL already has a list of challenges sections, each focusing on a cybersecurity topic. In order to establish the students who I am teaching, I focused on a student with at least three years in the Bachelor of Science in Computer Science, who is already taking three computer programming courses, advance computer programming course, and computer networks course, as shown in table 1.

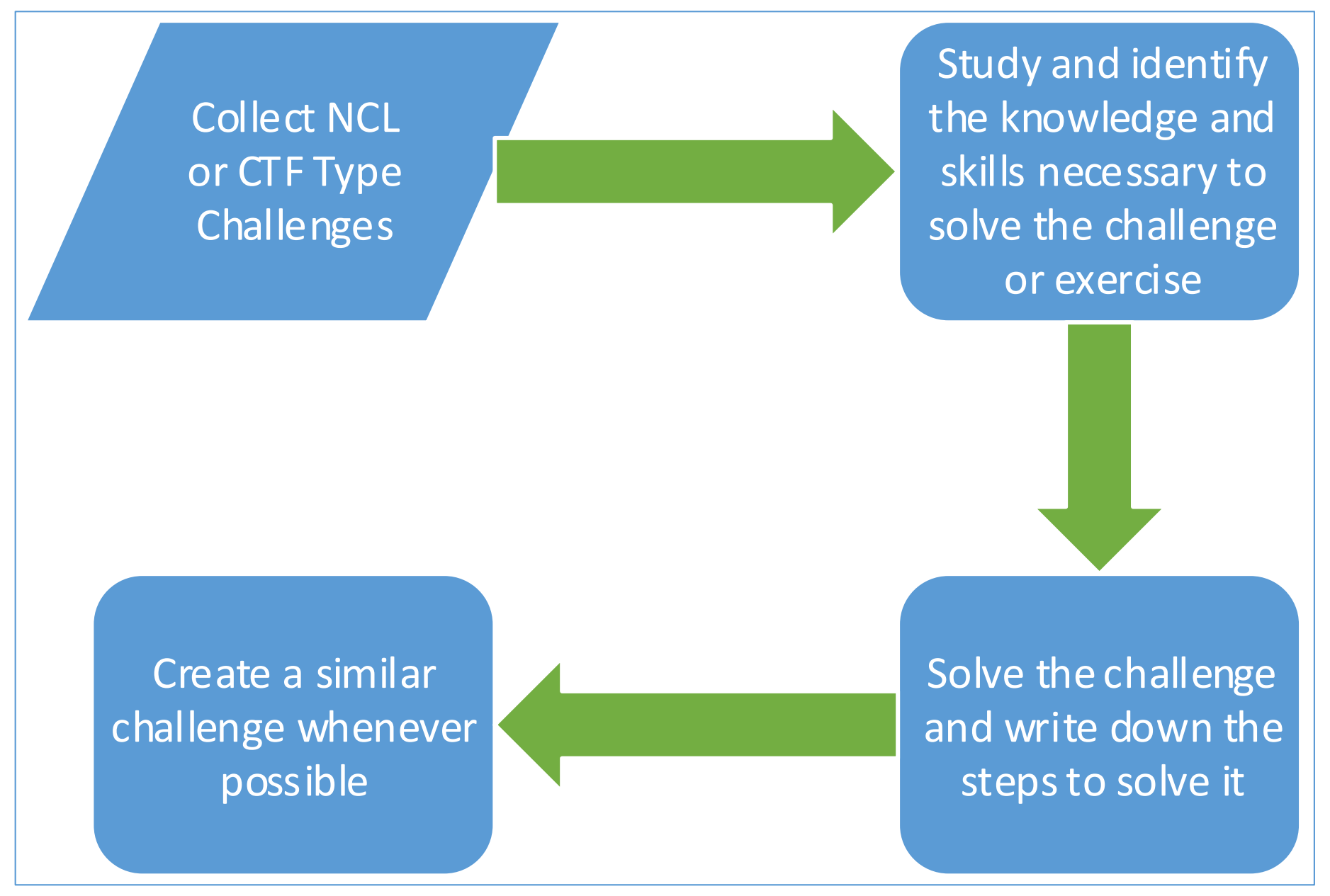
Course Code	Course Title
CECS 2200	Computer Programming Fundamentals
CECS 2202/2203	Computer Programming 1/Lab
CECS 2222/2223	Computer Programming 2/Lab
CECS 3210	Advance Computer Programming
COE 4330/4331	Computer Networks/Lab

Table 1. Courses Recommended

This way, the students taking the course will have the necessary computer science knowledge to understand most of the lab content, without the need for the lab to go too deep in computer science material. The end purpose of this project is to create the first prototype of the labs that will be used in a course or a set of workshops that, based on the feedback of the students and professor, could be tailored and changed until it becomes a better educational packet that can be integrated into other ongoing cybersecurity education initiatives.

One problem with this kind of project is generating new exercises, because some of them, like the network traffic analysis, depend on capturing network packets under a controlled network and replicating different types of network exploitation activities or downloading files that pose as malicious files. All of this require set ups that are more sophisticated and harder to implement. While other exercises are easier to create because they depend on files that can be manipulated by a single application with no need of complex set ups like a log file.

In order to generate more labs and exercises, it is essential to identify and study the skills and tools needed to solve each challenge. This will also help to create the step-by-step instructions that explain a tool or technique. It is important to show the student the output of the tools, as well as detailed instructions on how to use them.



Collect NCL or CTF Type Challenges

Study and identify the knowledge and skills necessary to solve the challenge or exercise

Solve the challenge and write down the steps to solve it

Create a similar challenge whenever possible

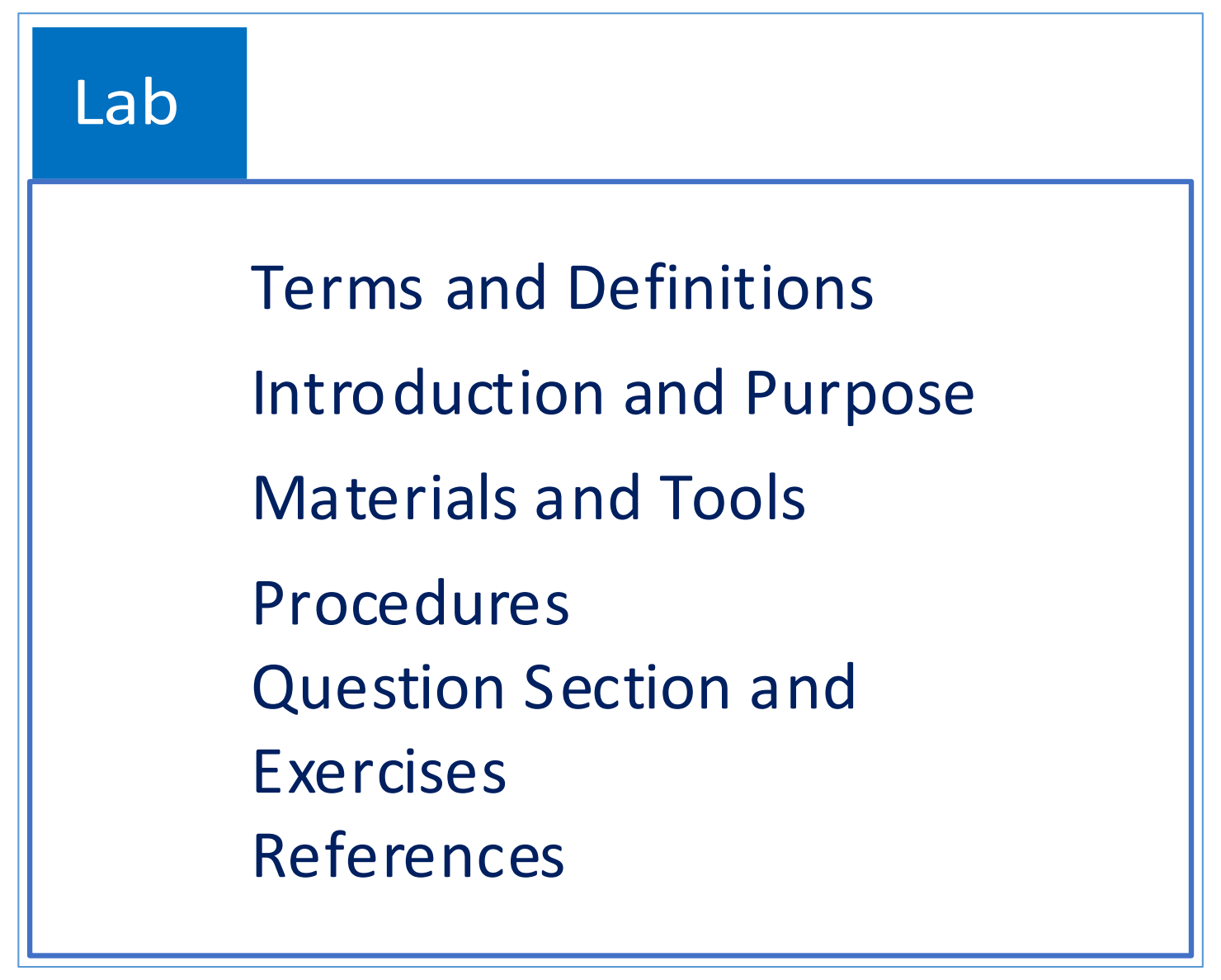
Fig. 1 Process to generate exercises

Outcome

I produced a total of eight labs, which were created using the NCL challenges as a guide, these are:

1. Cryptography
2. Enumeration and Exploitation
3. Log Analysis
4. Network Traffic Analysis
5. Open Source Intelligence
6. Scanning and Reconnaissance
7. Password Cracking
8. Wireless Access Exploitation

Each lab consists of the parts shown in figure 2.



Lab

Terms and Definitions
Introduction and Purpose
Materials and Tools
Procedures
Question Section and Exercises
References

Fig. 2 Lab Composition

Each lab was worked using a Kali Linux virtual machine, which will be part of the materials used by the students throughout the course; so all the students had the same chances of completing the labs by having the same tools at their disposition. Also, the virtual machine will contain the labs and the exercises to solve and answer the question section as shown in figure 3.

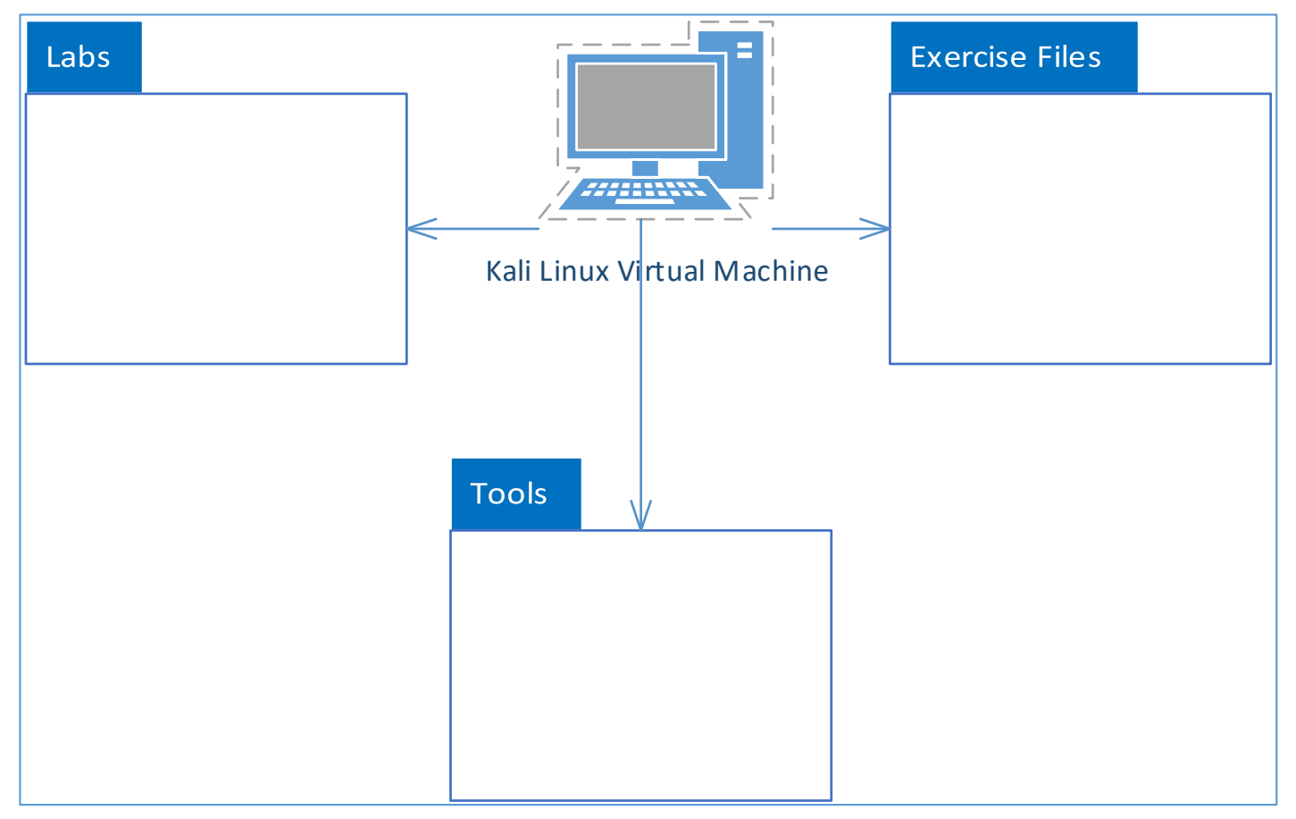
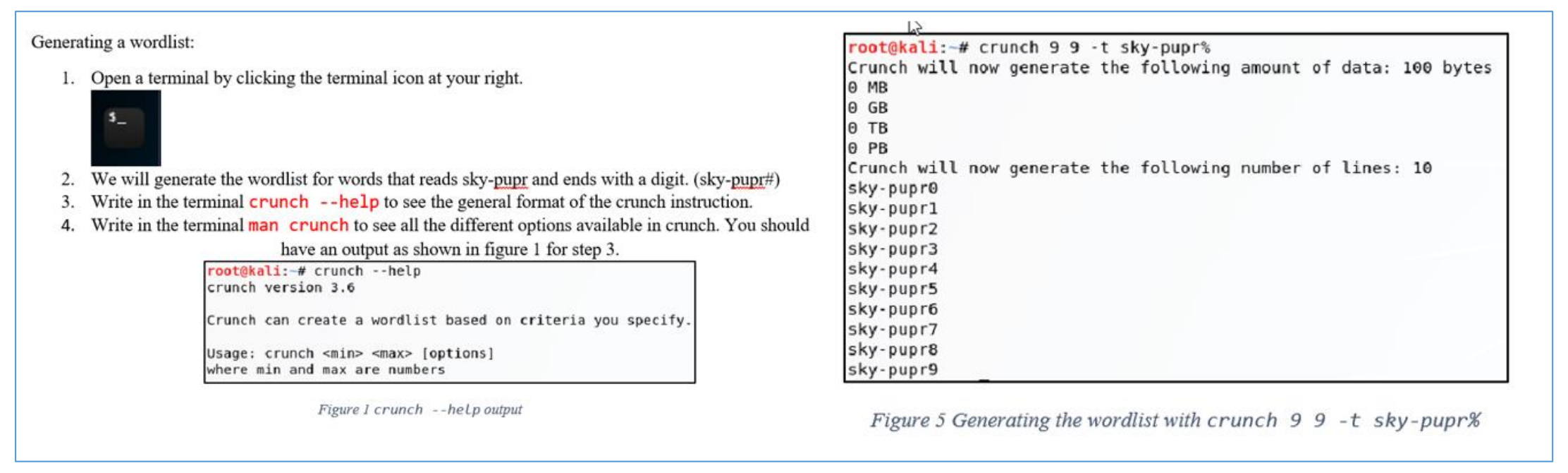


Fig. 3 Kali Linux Virtual Machine Content

All tools and topics are introduced with step-by-step examples the students can follow before they test their skills against the question section's exercises or the NCL challenges. Below in figure 4 you can see a sample of the content in the Password Cracking lab.



Generating a wordlist:

1. Open a terminal by clicking the terminal icon at your right.
2. We will generate the wordlist for words that reads sky-pupr and ends with a digit. (sky-pupr#)
3. Write in the terminal `crunch --help` to see the general format of the crunch instruction.
4. Write in the terminal `man crunch` to see all the different options available in crunch. You should have an output as shown in figure 1 for step 3.

```
root@kali:~# crunch --help
crunch version 3.6

Crunch can create a wordlist based on criteria you specify.

Usage: crunch <min> <max> [options]
where min and max are numbers
```

Figure 1 crunch --help output

```
root@kali:~# crunch 9 9 -t sky-pupr%
Crunch will now generate the following amount of data: 100 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10
sky-pupr0
sky-pupr1
sky-pupr2
sky-pupr3
sky-pupr4
sky-pupr5
sky-pupr6
sky-pupr7
sky-pupr8
sky-pupr9
```

Figure 5 Generating the wordlist with crunch 9 9 -t sky-pupr%

Fig. 4 Sample from the Password Cracking lab

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 use 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 Yoshuam Alicea and Steven Bennet for their work in 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 # 1563978.

References

[1] Tobey, D. H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers. *ACM Inroads*, *5*(1), 53-56.
[2] Burley, D. L. (2015). Cybersecurity education, part 1. *ACM Inroads*, *5*(1), 41.
[3] Burley, D. L. (2015). Cybersecurity education, part 2. *ACM Inroads*, *6*(2), 58-59.
[4] Leune, K., & Petrilli, S. J. (2017). Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. Proceedings of the 18th Annual Conference on Information Technology Education - SIGITE 17.
[5] Ford, V., Siraj, A., Haynes, A., & Brown, E. (2017). Capture the Flag Unplugged. Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education - SIGCSE 17.