8-10-2023

Developing Standards for Cybersecurity Labs

Glen Sagers
Southern Utah University, glensagers@suu.edu

Developing Standards for Cybersecurity Labs

TREO Talk Paper

Glen Sagers
Southern Utah University
glensagers@suu.edu

Abstract

Hands-on laboratory exercises in cybersecurity education are so important that both the IEEE/ACM 2017 curriculum guidelines (IEEE, 2017) and the National Centers of Academic Excellence (NCAE, formerly CAE) (NSA, 2020) curriculum requirements mandate the use of laboratory environments to allow students to practice the skills they learn in the classroom.

Labs take a great deal of time, expense, and technical knowledge to develop. Software, hardware, and the threat environments constantly change, meaning that maintenance is also a major task for instructors. Much has been written about ways to automate lab development and operation, but to date, there is virtually no literature that investigates whether labs that are developed in any computer fields are pedagogically effective. Similarly, little has been written about what makes any hands-on exercise effective. The discipline needs a framework or guidelines, based on sound instructional design and pedagogy, on how to develop labs that will best help students learn to implement skills.

In the engineering discipline, faculty have long recognized the need for laboratory instruction. In 2002, the question "How many engineering colleges or individual disciplinary programs have taken a comprehensive look at their laboratory experience?" (Feisel, 2002). This question does not appear to have been asked in computing or cybersecurity programs. The time has come, simply having lab exercises is not enough, they must be effective in teaching our mandated content.

Some specific issues with lab exercises that I have observed over 15 years include:

- Labs are often written by a single instructor. This may limit topic choices and technical quality.
- Student engagement may be lacking in lab exercises.
- Even an engaging lab may not be appropriate for the level of the course or the student preparation.
- A lab that is too detailed or too sparse in terms of instructions will limit student learning.
- Non-standard or proprietary tools may limit the applicability of skills learned in career settings.
- Many labs contain bugs, especially as software changes.
- The scope of the hands-on exercise may be inappropriate for the course or time allotted.
- Student collusion and cheating may be difficult to prevent in lab environments and exercises.
- Grading can be very time consuming.

This is certainly not an exhaustive list. It is vital that we, as faculty, make mandated labs as useful as we can. How can we develop guidelines for pedagogical effectiveness?

References

IEEE Computer Society and ACM, 2017. "Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," available at https://dl.acm.org/doi/book/10.1145/3184594

NSA (National Security Agency and Department of Homeland Security), 2020. "National Centers of Academic Excellence in Cyber Defense Education Program (CAE-CDE): Criteria for Measurement - Bachelor, Master, and Doctoral Level," available from: https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_designation_requirements.pdf

Feisel, L., and Peterson, G. 2002. "The challenge of the laboratory in engineering education," *Journal of Engineering Education* (91:4), pp. 367-368.