Creating Shareable Cybersecurity Laboratory Exercises

Wm. Arthur Conklin
waconklin@uh.edu

University of Houston, College of Technology
Houston, TX, USA

Abstract – Laboratory exercises are one of the foundational elements behind a hands-on, active learning curriculum. Creating these exercises in a manner that can be shared between institutions necessitates specific elements be addressed in the creation of the laboratory exercise. This paper examines these elements and how they support a shareable laboratory experience that can be easily replicated between programs.

Keywords

Cybersecurity, Laboratory exercises, active learning

1. INTRODUCTION

The fact that there is a shortage of information security professionals is known by all involved.[1] Educators, employers, governments, the consensus is clear, we need more trained personnel. The correct path to solve this problem is less clear, with many different organizations offering solutions, from the US Government sponsoring scholarships and recognizing education programs, to industry offering boot camps to new employees with proven aptitudes.[2-7] Virtually all of these solutions share some common attributes, one of the more important being the inclusion of hands-on exercises to support active learning.[8]

The field of cybersecurity is relatively new, roughly 50 years old, and being a sub-discipline of several disciplines, one where boundaries and foundations are still under development. The breadth of cybersecurity includes everything from a technical computer science/computer engineering perspective, to business, to psychology of actors, to policy, to law and more. This breadth causes issues when content for one aspect is conflated or substituted for another aspect of the overall discipline. This paper is focused on the technical activities that are used to attack and defend information systems as part of a cybersecurity effort.

Active learning is a term used to describe a set of instructional methodologies designed to actively engage the student in the learning process. There are a whole slew of specific methods, from group projects, to demonstrations, to case work, to, yes, laboratory exercises.[9] Active learning is designed to create an environment for deeper learning, and for learning of tasks higher up the Bloom's taxonomy. Where as knowledge-based learning involves memorization and recall, active learning creates an environment more suited for tasks such as application, analysis and evaluation.[10]

Cybersecurity laboratory exercises are just one example of applied active learning techniques, but they can be particularly effective in developing the skills needed for working as a cybersecurity professional. Laboratory exercises can be used to reinforce elements shown during lectures, or to introduce actual

work tasks performed by professionals. The key to developing useful labs is to identify the true purpose of the laboratory exercise from a student objective point of view, rather than just doing things to be doing things. This connection to meaningful learning objectives is one of the key elements in separating great labs from those that only use time and resources.

The other key elements in creating a useful and meaningful lab include clear instructions to the student, and checkpoints along the way to ensure that the student does not end up astray and in a situation that does not reinforce learning objectives. Questions and answers along the way provide meaningful checkpoints, and assessment opportunities.

The creation of good laboratory exercises can take substantial resources to create and maintain. One of the most challenging aspects of cybersecurity laboratory exercises is the creation of appropriate datasets to support the learning objectives. These datasets range from packet captures, to system images, to specifically crafted systems to be susceptible or demonstrate key activities. Once developed and vetted through troubleshooting, a dataset/laboratory exercise is a valuable item, not a commodity, and one that many academics would want to borrow/share/reuse. For sharing to be effective, there are several key considerations that should be addressed and documented, preferably when the laboratory exercise is developed. These elements are described in detail in the next section.

2. REQUIREMENTS

If an institution is going to adopt another institution's laboratory exercises and include them in their own curriculum, then there are some key items that need to be described up front before they can be integrated. Some of the items are administrative in nature, the name of the lab, details on pre-requisites, how long the lab takes, etc. Others are critical for proper integration into a curriculum, such as learning objectives and details associated with the assignment. The last set of details are practical in nature, such as specific

directions, answers to questions and setup instructions to be used when setting up the lab. Each of these will be covered in detail in the following sections.

2.1 Administrative details

The administrative details of a laboratory are just that, information that is needed to use a lab. There are several elements, some of their uses are obvious, such as the name of the lab, the creator of the lab, and contact information. A description of the lab is useful, providing a simple explanation of the length and scope of the laboratory exercise. A description of the operating environment for the laboratory, if relevant, can help a potential adopter decide early on if the laboratory exercise fits within their system.

The level of student for which the laboratory exercise is targeted as well as any pre-requisite knowledge needed on the part of the student. Is the lab designed for individual or group student participation? A description of the student deliverables could prove useful for adoption decisions. This section is meant as a brief introduction to help a potential adopter make an early decision as to read on or choose another laboratory exercise. Additional, in-depth details will be provided in subsequent items.

2.2 Technical details

Technical details are a deep dive into specific technical details of elements associated with an exercise. Specific list of elements, folder names, file names, sizes, hash values, and dates are important for a variety of uses. Organizing these folders and the files contained within in a manner that makes their use easier. Having self-organizing structures such as numbered elements can significantly improve usability.

Technical details can include security data to allow for source code integrity checks of the files. Hash values for entire folders can be a fast

method of determining integrity issues. Technical data can also include warnings in the event of data elements that will trip anti-virus programs. Understanding and knowing these things before downloading critical files can go a long way to prevent extra work on the part of the adopter.

2.3 Learning Objectives

Learning objectives are the foundational element from the educational perspective. As the learning outcomes are the foundation for the what and why in the laboratory exercise, they must be clear, concise, and actionable by the student completing the lab. It is important that the learning objectives are appropriate to the level of instruction and to the desired level of Bloom's taxonomy. Learning objectives should be structured in a manner which makes them stackable and progressive through the material and the levels of Bloom's taxonomy to drive more complete learning outcomes. The learning objectives should be traceable through the lab material to points of learning within the lab.

2.4 Student materials

The student materials are the centerpiece of a laboratory exercise. The laboratory instructions for the student must be clear and aligned with learning objectives. This does not mean the all labs need step-by-step instructions, but rather the level of instruction should fir the level of student ability, the objective of the lab and the materials given.

A laboratory exercise by itself is an example of an active learning method, adding elements such as questions throughout the progressive steps of the laboratory can further engage the student and add to the active learning content. These questions should focus on the learning objective attainment, not just be placeholders for progress through the steps of the laboratory procedure.

2.5 Instructor materials

Instructors also need a complete set of laboratory materials, preferably annotated to provide information where students get stuck, or at key points where learning activities might require assistance. A complete set of answers to all questions, including how to get to the answers will assist in the instructor or TA managing the activity as students perform the tasks associated with the laboratory procedure. A rubric to manage the answer key to questions will assist in the grading efforts.

Having a complete guide to all of the materials in the laboratory, the technical details, the set-up details, the operational details, all annotated and cross referenced will assist in the use of the laboratory. The objective of this information is to make it easy for the instructor to assist in the attainment of the learning objectives by students.

2.6 Lab technician materials

Installing labs is a lot like installing software packages on a computer system. There can be issues with having the correct platform, the correct libraries, getting the installation correct and troubleshooting problems during installation. A key element for seamless lab adoption is a comprehensive installation guide for the person who will be instantiating the lab exercise. For some labs, this will be as simple as supplying a datafile to students and letting them run their own tools. Other cases may involve VMs that can be run. Some cases may require extensive setups or multiple operating systems across multiple machines/VMs. In each case, it is incumbent upon the lab developer to provide setup instructions including methods of testing the setup.

2.7 Dataset

Not all laboratory exercises need specific datasets, or customized elements such as virtual machines (VMs). Where they are employed, there are two approaches to them: black box or white box. A black box data set is one where there no knowledge on how it is built. In these cases, one has to trust and use the dataset as given. In a white box case, the details of how to create the dataset are included. This method can provide information that can be used as part of the learning experience as well as setup and troubleshooting.

2.8 Material Source Control

For all the same reasons that enterprises use versioning and source control mechanisms these tools should be used on laboratory original source materials. When laboratory exercises are deployed there are risks of damage to the source materials. Maintaining a pristine source copy is essential when things go wrong and it is needed.

3. REPOSITORIES

When a laboratory is complete, there exists the question of how to share it with other instructors and other institutions. There are two methods, direct transfer and the use of a repository. Direct transfer is a 1:1 transfer of the information, from instructor to instructor. This method suffers from scale, as it requires a multitude of 1:1 interactions and for the developer of the lab to distribute to N schools, requires N interactions on the developer side as well as on the receiving side.

The use of a repository can alleviate a lot of work on the developer side. One upload can facilitate virtually unlimited downloads. The only challenge is keeping the repository up to date, a responsibility of the developer as the lab elements change over time. An example is the CLARK repository, clark.center, an NSF initiated digital library of cybersecurity learning objects.

The key advantage to a repository can be one stop shopping when looking for labs, including services such as indexing and peer reviews.

4. CONCLUSIONS

Developing and sharing laboratory exercises is a key tool for advancing cybersecurity education. With limited instructors, and lab development being a resource intensive undertaking, sharing the products is the sane path forward. In communities, such as the Centers of Academic Excellence in Cyber Defense education, sharing of curricular elements is a mandated element between member institutions. The objective of this paper was to examine what a shared item should contain for the greatest utility. While these steps may seem to add significant overhead to the development of a laboratory exercise, this level of detail makes all the difference when adoption decisions are being made. And this is clearly a case of build once and use multiple times.

REFERENCES

[1] Burning Glass, "Job Market Intelligence: Cybersecurity Jobs, 2015," D. Restuccia, Ed., ed, 2015.

[2] M. J. Assante and D. H. Tobey, "Enhancing the cybersecurity workforce," *IT professional,* vol. 13, pp. 12-15, 2011.

[3] R. Dodge, C. Toregas, and L. J. Hoffman, "Cybersecurity Workforce Development Directions," in *HAISA*, 2012, pp. 1-12.

[4] L. Fourie, S. Pang, T. Kingston, H. Hettema, P. Watters, and H. Sarrafzadeh, "The global cyber security workforce: an ongoing human capital crisis," 2014.

[5] C. R. Fuller, "Shortening the skills gap: An exploratory study of cybersecurity professional experience," Capella University, 2016.

[6] J. S. Galliano, J. O. WEBB JR, S. FONSECA-LIND, and K. M. HARGISS, "Improved Matching of Cybersecurity Professionals' Skills to Job-Related Competencies: An Exploratory Study," 2017.

[7] L. Hoffman, D. Burley, and C. Toregas, "Holistically building the cybersecurity workforce," *IEEE Security & Privacy,* vol. 10, pp. 33-39, 2012.

[8] D. H. Tobey, P. Pusey, and J. Chin, "Cybersecurity Competitions in Education: Engaging Learners through Improved Game Balance," in *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, 2015, pp. 99-100.

[9] M. Silberman, *Active Learning: 101 Strategies To Teach Any Subject*: ERIC, 1996.

[10] F. K. Weigel and M. Bonica, "An Active Learning Approach to Bloom's Taxonomy: 2 Games, 2 Classrooms, 2 Methods," *US Army Medical Department Journal,* 2014.