A Comparison of Two Hands-On Cybersecurity Frameworks*

Conference Tutorial

Jens Mache[1] *and Richard Weiss*[2]
[1]*Lewis & Clark College*
Portland, OR 97219
{jmache,author}@lclark.edu
[2]*The Evergreen State College*
Olympia, WA 98505
{weissr,author}@evergreen.edu

Abstract

There are several different frameworks for teaching hands-on cybersecurity exercises. Faculty who want to integrate cybersecurity into their courses may have difficulty in choosing one. In this tutorial, we will show faculty two different frameworks so that they can understand the possibilities. It is not necessary to choose only one. In our courses, we have taken advantage of multiple frameworks, in order to benefit from their individual strengths. We think this will lower the barrier for use.

In this tutorial, we will introduce the DeterLab and EDURange frameworks, and present one hands-on exercise from each. Participants try them, and discuss how they can be used in their courses.

1 Overview

Student exposure to practical, hands-on exercises is critical for cybersecurity curricula. It helps students internalize concepts taught in class, learn to use cybersecurity tools, and learn critical and adversarial thinking.

EDURange [1, 4, 5, 6, 7, 8] is a cloud-based framework for cybersecurity exercises designed with three major goals. First, ease-of-use for students and instructors. Scenarios run on VMs that are created automatically in the public cloud. Students don't need special software and can work anywhere with

Internet service. Instructors can register their classes. Students can work in groups. EDURange collects data to make assessment easier. Second, engaging for students and faculty. Students from a variety of backgrounds can learn practical security concepts, tools, and skills in scenarios that gamify realistic challenges. Third, flexibility. Use simple scripts to specify exercises at a high level and create variations. This enables instructors to tailor exercises to their specific classes and student backgrounds and continue to modify them in order to minimize risk of students finding the answers online.

DeterLab [2, 3] is both an educational and a research platform on a private cloud. Once the instructor reserves resources for their class, students have control over starting and stopping their "experiment". Similar to EDURange, there are scripts that install the OS and required software packages. DeterLab has a variety of "homework" exercises, available via the education portal [2], cover a wide range of topics including: buffer overflows, code injection and command-injection attacks, man-in-the-middle attacks, worm modeling and detection, botnets, router and DNS attacks, and DDoS attacks. Each of these exercises is a packaged experiment that demonstrates one of these topics, providing students with direct observation of attacks and interaction with targets. Students create and manipulate an instance of an experiment and follow the instructions to demonstrate attacks and defenses, and improve their practical cybersecurity skills. Both DeterLab and EDURange rely on the command line interface and have the ability to capture and analyze student interactions.

2 Acknowledgements

This work was partially supported by National Science Foundation grants 1723705, 1723714, 1516100 and 1516730.

References

[1] `https://edurange.org/scenarios.html`, accessed July 2019.

[2] `https://www.isi.deterlab.net/sharedpublic.php`, accessed July 2019.

[3] J. Mirkovic and T. Benzel. Teaching Cybersecurity with DeterLab. *IEEE Security Privacy*, 10(03):73–76, 2012. doi: `https://doi.ieeecomputersociety.org/10.1109/MSP.2012.23`.

[4] R. Weiss, S. Boesen, J. Sullivan, M. E. Locasto, J. Mache, and E. Nilsen. Teaching cybersecurity analysis skills in the cloud. In *Proceedings of the 46th ACM Technical Symposium on Computing Science Education*,

SIGCSE '15. ACM, 2015. doi: http://dx.doi.org/10.1145/2676723.2677290.

[5] R. Weiss, M. E. Locasto, and J. Mache. A reflective approach to assessing student performance in cybersecurity exercises. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, SIGCSE '16, pages 597–602. ACM, 2016. doi: http://dx.doi.org/10.1145/2839509.2844646.

[6] R. Weiss, J. Mache, and M. E. Locasto. The EDURange framework and a movie-themed exercise in network reconnaissance. In *Proceedings of USENIX Security: Advances in Security Education Workshop*, ASE, 2017.

[7] R. Weiss, F. Turbak, J. Mache, and M. E. Locasto. Cybersecurity education and assessment in EDURange. *IEEE Security Privacy*, 15(3):90–95, 2017. doi: http://doi.ieeecomputersociety.org/10.1109/MSP.2017.54.

[8] R. Weiss, F. Turbak, J. Mache, E. Nilsen, and M. E. Locasto. Finding the balance between guidance and independence in cybersecurity exercises. In *USENIX Workshop on Advances in Security Education*, 2016.