

Cybersecurity Exercises in the Age of LLMs

Conference Tutorial

Richard Weiss¹, Jens Mache²

¹The Evergreen State College, Olympia, WA 98505

`weissr@evergreen.edu`

²Lewis & Clark College, Portland, OR 97219

`jmache@lclark.edu`

In this tutorial, we will introduce a cybersecurity education framework for developing polymorphic hands-on exercises. Many faculty readily acknowledge the importance of cybersecurity in the Computer Science curriculum, but there are still barriers to integrating it into existing courses. One of those barriers is the fact that in most courses, the current content fills the entire term. Another issue is that faculty don't have time and expertise to create new content that would fit well with their current content and style. The third problem is that exercises created should be resistant to solution by LLMs. We have developed cybersecurity exercises that combine two principles: environment specificity and polymorphism. Environment specificity means that the solutions to the exercise should depend on the local environment (LLMs don't have access to that information). In this context, polymorphism means that they can be easily modified each time that the class is taught.

Overview

EDURange [2, 6, 3, 7, 5] has been developed over more than ten years, and it continues to evolve. We have used it to integrate hands-on security exercises in our own classrooms and will present our exercises and framework that satisfy the two principles: environment specificity and polymorphism. The exercises that we will describe are relevant to: introductory courses that use the Linux command line, Operating Systems, Computer Networking, Database Systems. We will also demonstrate the feedback system that we have added that allows instructors to interact with students one on one [9, 4, 8, 1].

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. 2216485 and 2216492.

References

- [1] Aubrey Birdwell, Jack Cook, Richard Weiss, and Jens Mache. From logs to learning: Applying machine learning to instructor intervention in cybersecurity exercises. In *Proceedings of the American Society for Engineering Education (ASEE) Annual Conference*, 2024.
- [2] Jack Cook, Richard Weiss, Jens Mache, Carlos García Morán, and Justin Wang. An authoring process to construct docker containers to help instructors develop cybersecurity exercises. *Journal of Computing Sciences in Colleges*, 37(10):37–47, 2022.
- [3] Jelena Mirkovic, Aashray Aggarwal, David Weinman, Paul Lepe, Jens Mache, and Richard Weiss. Using terminal histories to monitor student progress on hands-on exercises. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, pages 866–872, 2020.
- [4] Quinn Vinlove, Jens Mache, and Richard Weiss. Predicting student success in cybersecurity exercises with a support vector classifier. *Journal of Computing Sciences in Colleges*, 36(1), 2020.
- [5] Richard Weiss, Stefan Boesen, James F. Sullivan, Michael E. Locasto, Jens Mache, and Erik Nilsen. Teaching cybersecurity analysis skills in the cloud. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, 2015.
- [6] Richard Weiss, Franklin Turbak, Jens Mache, and Michael Locasto. Cybersecurity education and assessment in edurange. *IEEE Security & Privacy*, May/June, 2017.
- [7] Richard Weiss, Franklin Turbak, Jens Mache, Erik Nilsen, and Michael E Locasto. Finding the balance between guidance and independence in cybersecurity exercises. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*, 2016.
- [8] Valdemar Švábenský, Kristián Tkáčik, Aubrey Birdwell, Richard Weiss, Ryan S. Baker, Pavel Čeleda, Jan Vykopal, Jens Mache, and Ankur Chattopadhyay. Detecting unsuccessful students in cybersecurity exercises in two different learning environments. In *Proceedings of the IEEE Frontiers in Education Conference (FIE)*, 2024.
- [9] Valdemar Švábenský, Richard Weiss, Jack Cook, Jan Vykopal, Pavel Čeleda, Jens Mache, Radoslav Chudovský, and Ankur Chattopadhyay. Evaluating two approaches to assessing student progress in cybersecurity exercises. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education*, 2022.