Abstract

Educating Cyber Defenders: Technical Challenges in Designing Scalable Hands-on Learning Systems

Author: Margus Ernits (Margus.Ernits@gmail.com)

Keywords: Teaching Cybersecurity, Hands-on Learning, Problem-Based Learning

Hands-on, problem-based learning has proven to be an effective method for teaching cybersecurity due to its realism and engaging activities. Several hands-on learning systems focus on offensive techniques, such as Capture the Flag (CTF) competitions, as well as defensive exercises like Cyber Defense Exercises (CDX), large-scale live-fire exercises, and forensic challenges. However, what are the technical challenges in creating a scalable, defense-oriented cybersecurity learning system? Why do most existing defense-oriented systems focus primarily on identifying Indicators of Compromise (IOC) or forensic findings? How can a cyber defense-oriented learning system be designed where defenders not only identify threats based on log files or forensic evidence but also respond to live-fire events as a team? This is common for large scale technical exercises and it is difficult to downscale or scale for massive online learning cases. In this paper we propose a technical architecture and methods for a scalable defense oriented online learning system. The proposed system architecture has been tested in over 100 live-fire team exercises and approximately 700,000 online learning sessions.