From training to education: Lessons learned in building academic curriculum from industry leading security training.

Abstract: Although understanding the offensive (hacking) side of cyber security is an important aspect to building defensible and secure systems, very few institutions offer offensively focused courses. Developing a robust offensive curriculum is difficult because of the large infrastructure requirement, the breadth of the subject matter, and the fast pace evolution of the material. To enable easier development of offensive curriculum, this paper analyzes a two-year pilot course that utilized a hybrid approach to offensive security education by combining industry leading training with the tenants of academia. This pilot leveraged the established framework and real-world applicability of modern certificate training to ensure the relevance of the curriculum. The pilot also incorporated the elements of gamification throughout the course to foster teamwork and enhance the students' motivation. This motivation helped the students persevere through the difficult, frustrating, and sometimes time-intensive problem-solving process required by the curriculum. Finally, the course leveraged the academic environment to improve on the existing course material by answering the "why" and "how" that is missing in the more narrowly-focused certificate training that is primarily focused on the "what". This "why" greatly improved the students' ability to troubleshoot and apply the demonstrated techniques to new and unique scenarios. Ultimately, this pilot course found that, by applying an education mindset to successful industry training, one can build a robust academic curriculum that combines the benefits of both programs to create a more instructional classroom experience for your students.

More Details: I developed and taught a two-year pilot course at the United States Military Academy (West Point) based on Offensive Security's Penetration Testing with Kali Linux (PWK). PWK is the preparatory course for the Offensive Security Certified Professional (OSCP) certification, one of the leading (if not the leading) offensive certifications. In this presentation, I will walk through this pilot course from development to execution and examine the results. In particular, I will provide examples of topics covered in the base PWK training that were frustrating for the students and demonstrate how, by explaining how the underlying technologies worked (the education approach), the students were able to better understand the training tasks. They then leveraged this new found understanding to troubleshoot more advanced problems. I will also explain the various gamification methods used in the course and discuss how these methods furthered enhanced the students' understanding of the material. Attendees will leave this presentation with an appreciation for how to leverage modern certification training to improve academic courses and with an initial blueprint for how to establish an offensively focused course at their institution.