RMS ASEE 2019 Poster (Extended Abstract) Guidelines

Abstract: Students rely largely on class lectures and assignments to refine their skills and prepare themselves for their future careers. However, success in the workplace depends on each individual's ability to transfer their academic knowledge to professional occupations. The opportunity for authentic experiences, specifically modeling real world jobs, enables students to learn important skills through hands-on practice. These experiences allow students to learn common pitfalls and complications before they start working for a company. In cybersecurity, this could mean the difference between defending a company's system against intruders and a security breach. With security threats becoming more prevalent and increasingly complex, professional success hinges on the ability to refine student's skills in a controlled environment before they enter the workforce. Cybersecurity competitions provide these controlled environments and facilitate learning. Crucial to students preparing for their future careers, cybersecurity competitions garner student interest, get students involved in extra research opportunities, and bring enjoyment to tasks that would be difficult to learn on the job. Additionally, competitions empower students to balance education and experience and empower companies to hire applicants with a mastery of complex subject matter as well as real world experience. Competitions help students see who they will be competing against for jobs in the future and show students where they have room for improvement. Our research lab has found that students involved in competitions are more interested and more involved in cybersecurity and better equipped for the workplace.

EXTENDED ABSTRACT (Max 2 Pages)

Cybersecurity competitions provide the opportunity for tangible experience in detecting prevailing cyber attacks and employing effective defensive responses. These extra-curricular provide a unique experience for students [1]. These activities encourage collaboration and provides necessary preparation for security professionals, giving students the chance to work in effective groups in an environment similar to one they can expect after graduation. Additionally, these competitions can be sculpted and perfected to provide the best experience to the students and amplify learning.

Participation

Three main cybersecurity events were entertained. First, six students participated in an attack-and-defense competition to gauge their skill level with others from different schools. Attack-and-defense competitions pit blue team system defenders against red team system attackers. This provides hands-on experience for applications in information security. Second, thirty-five students participated in a jeopardy-style competition over multiple weeks. Jeopardy-style competitions allow for more controlled environments and minimize the necessary computer science background knowledge required to succeed. Third, six students participated in a second attack-and-defense competition to determine the consistencies and inconsistencies among competition platforms.

Collaboration

Cybersecurity experts commonly work in teams with clearly defined roles. This allows for the team to accomplish more than the cumulation of each individual working separately. Collaborating with teammates, particularly when each team member has a specialized role, leads to higher success rates during competition [2]. Teamwork (and similar soft skills) can be transferred to other classes, jobs, and activities and leads to more creative solutions. Additionally, since these competitions are voluntary, it gives students the unique opportunity to participate in highly-interactive group work.

Preparation

Class lectures and assignments do not properly prepare students for careers in a dynamic cybersecurity landscape. Theoretical knowledge, while critical to forming a complete understanding of various topics, does not apply simply or directly to actual professional systems. Transferring academic knowledge to professional settings slows progress and keeps young professionals from achieving goals equivalent to their potential. To build these skills and develop their expertise in cybersecurity, young professionals must seek out other opportunities beyond their classes to accompany their theoretical academic knowledge.

Engaging students in truly extra-curricular activities facilitates the growth of crucial skills for successful cybersecurity careers. Cyber defense depends on the ability of system defenders to react appropriately to different types of attacks across different platforms with varying degrees of severity [2]. Making these decisions requires experience and effective teamwork. Owning such experience through competitive team-based opportunities gives new professionals the chance to refine their abilities before completing their education.

Advancements

Successful cybersecurity competitions provide students the opportunity to gain relevant experience in addition to their coursework. By perfecting their skills early, they are more likely to succeed in their future careers. These experiences teach students prevalent attacks and appropriate defenses before beginning their work.

Cybersecurity competitions provide controlled environments which allows for events to occur at ideal (or nonideal) times. These competitions are not trivial to run however. Specific environments allow for optimal learning and exceptional experiences. Advancements have been made to administering cybersecurity competitions, including efforts to generate virtual machines automatically [3], entertaining higher-level simulations for security training.

REFERENCES

[1] C. Eagle, "Computer Security Competitions: Expanding Educational Outcomes," in *IEEE Security & Privacy*, vol. 11, no. 4, pp. 69-71, July-August. 2013.

[2] N. Buchler, G. G. La Fleur, B. Hoffman, P. Rajivan, L. Marusich, and L. Lightner, "Cyber Teaming and Role Specialization in a Cyber Security Defense Competition," in *Frontiers in Psychology*, vol. 9, no. 2133, November 2018.

[3] M. Sanchez Rubio, G. Lopez Civera and J. J. Martinez Herraiz, "Automatic Generation Of Virtual Machines For Security Training," in *IEEE Latin America Transactions*, vol. 14, no. 6, pp. 2795-2800, June 2016.