Chapter 87
Cyber Defense Competitions as Learning Tools:
Serious Applications for Information Warfare Games

Julie A. Rursch
Iowa State University, USA

Doug Jacobson
Iowa State University, USA

ABSTRACT

In a cyber defense competition, students design, configure, and maintain a set of servers and a network in a secure manner. The students' goal during the competition is to prevent security breaches and to remediate any exploits that occur while maintaining a fully functional network for their end users. Cyber defense competitions provide active student learning, mimic real-world situations, and provide engagement with computer and network security topics. To date, Iowa State University has hosted 18 cyber defense competitions across four divisions: high school students, community college students, ISU students, and four-year university students from across the nation. This chapter provides a brief history of cyber defense competitions, as well as describes how they are run. The authors also address the needs of different audiences who participate in cyber defense competitions and show that beyond building and strengthening computer and network security skills, cyber defense competitions can be used for recruitment, retention, advanced training, and experimentation for students.

INTRODUCTION

Cyber defense, as well as protection of other critical infrastructures, is at the forefront of security professionals' agendas, as well as the nation's psyche. The ongoing release of new viruses, day one attacks and the threat to our national infrastructure, including Supervisory and Control and Data Acquisition (SCADA) systems, demonstrates the need for professionals trained in the science, as well as the art, of cyber defense and computer and network security.

DOI: 10.4018/978-1-4666-4707-7.ch087

Several institutions of higher education offer degrees in information assurance or computer and network security. These programs generally teach at least one course in information warfare or information assurance where students conduct lab experiments that demonstrate current security vulnerabilities and allow students to exploit those vulnerabilities in a controlled manner. Some programs, ours at Iowa State University (ISU) included, provide a break-in laboratory which allows students several weeks to attack a dummy corporation's network in an attempt to understand how an attacker may use social engineering, software or application vulnerabilities and brute force to gain access to systems, networks, databases and corporate documents.

While these classes are useful and provide training to many four-year students, we have found that cyber defense competitions develop additional skills and a deeper understanding in computer and network security than coursework does alone, even when labs as described above are included. Students who compete in cyber defense competitions not only gain knowledge, but also increase their interest in working in the cyber security area. They also receive real world experience in configuring and protecting a network just as security professionals do on a daily basis. At ISU, we run four cyber defense competitions per year for students. One each for Iowa high school, Iowa community college (two-year), ISU students and four-year students from universities across the nation. To date we have run 18 cyber defense competitions with more four more planned for 2011. While participation varies from 40 to 175 depending upon the event, we have had nearly 1350 students participate in cyber defense competitions over the past five years. We also run cyber defense competition/security workshop combinations for Information Technology professionals who are tasked with ensuring security for computer and network system, as well as Computer Science or Information Technology faculty who want to learn more about security and running their own cyber defense competitions. We have found these individuals also benefit from the ability to learn and work, as well as test out new attack and defense mechanisms, in a controlled environment.

This book chapter provides a brief history of cyber defense competitions, as well as describes how they are run. It also addresses the needs of different audiences who participate in cyber defense competitions. This chapter demonstrates that beyond building and strengthening computer and network security skills, the cyber defense competitions can be used for recruitment, retention, advanced training and experimentation for students. The audiences that will be covered include high school students, community college students, four-year university students and Information Technology professionals and faculty.

BACKGROUND

Cyber defense competitions have various incarnations from capture the flag competitions where students try to earn entrance into systems and gain access to specific files to competitions where students defend sets of systems that either they configure or have been preconfigured for them. Although there are competitions where students are allowed to play both defensively, protecting their own systems, and to launch an offense, attacking other competitors' systems (Vigna, 2003), a larger portion of cyber defense competitions only allow students to take the defensive approach. From a historical perspective, cyber defense competitions where students provide a defense only position against their attackers can trace their beginnings to the Cyber Defense Exercise (CDX) which was first held in 2001. The competition was conceived by representatives from the U.S. Military Academies as a event where participating academies would compete against each other in defending their network against security professionals playing the role of attackers. It was designed to serve as a final project for students majoring in computer