Abstract:

Across the US and the rest of the world, there exists a lack of computer security components in many CS/IT curricula. For those programs that do have such components in computer security, a common difficulty is to integrate "real-world" labs into the courses, in order to provide hands-on experiences to the learners. Due to concerns for security breaches and network hacking, system administrators are reluctant to allow computer security labs involving network sniffing, virus scripting, etc. to be deployed in the campus network. Without hands-on, real-world projects, it is difficult for the learners to integrate the acquired security theories and knowledge with up-to-date security technologies and practices. Computer science educators who are interested in teaching computer security in a "realistic" context are thus faced with a unique challenge: Setting up 'real-world' computer security laboratories and assignments, without negatively impacting the rest of the campus network. The primary goal of our project is to develop a Distributed Computer Security Lab (DCSL) to answer the challenge. We have established, across multiple university campuses, a computer lab which enables the faculty and students to analyze and study vulnerabilities of a realistic corporate network. The lab provides hands-on experience for students to study cutting-edge computer security technologies, and serves as a test bed for projects which are otherwise impossible to implement in general-purpose labs. In this paper, we first discuss the general model of the DCSL and our implementation, and then present a selected set of projects that we have conducted to aid the design of the DCSL. The paper concludes with a summary and future work.

Citation:

Yang, A., Yue, K., Liaw, M., Collins, G., Venkatraman J., Achar, S., Sadasivam, K., and Chen, P., Design of a distributed computer security lab, Journal of Computing Sciences in Colleges. Volume 20, Issue 1. pp. 332-346. 2004.