TEACHING CYBERSECURITY THROUGH GAMES: A CLOUD-BASED APPROACH *

TUTORIAL PRESENTATION

Richard Weiss
The Evergreen State College
Olympia, WA 98505
weissr@evergreen.edu

Michael Locasto
University of Calgary
Calgary, Alberta, Canada
locasto@ucalgary.ca

Jens Mache
Lewis & Clark College
Portland, OR 97219
jmache@lclark.edu

Vincent Nestler
California State University, San Bernardino
San Bernardino, CA 92407
nestlerv@mac.com

ABSTRACT

Incorporating information security into the undergraduate curriculum seems to be a topic of growing interest to CCSC-NW attendees. In addition, it is receiving increased attention nationally in the proposed ACM/IEEE CS2013 Curricula Guidelines [1]. This area will be one of the new core requirements. The goal of this workshop is to provide faculty who have little experience in this area with some of our most recent tools and resources that would facilitate their incorporating this knowledge area into their curriculum. It builds on previous similar workshops in this area. In this tutorial, we will describe the use of cloud-based environments for developing and disseminating hands-on security exercises. We present one security game that we have developed on Amazon's AWS cloud environment and an exercise that was developed on The RAVE. Participants will learn about the framework we have developed for providing instructors with competitive, interactive exercises through the system EDURange[2]. EDURange is a new framework for creating exercises and games in a variety of environments including remotely hosted web services, i.e. cloud computing. They will learn about these exercises from two viewpoints. As players, they will learn about network security. As instructors, they will learn how to use these security exercises in the classroom, and they

will learn about the scenario description language, which they can use to create games for their classes.

OVERVIEW

We have chosen one exercise that can be played as a game, and which could be used by any computer science faculty with a little training. The objectives of our workshop are: 1) to introduce the EDURange framework for creating competitive, interactive exercises; 2) to describe The RAVE environment, which allows faculty to set up and manage virtual networks for their students; and 3) have faculty try a security exercise, and discuss how it can be adapted to a variety of courses that they teach.

EDURange implements a scenario description language (SDL). This allows instructor to create a security game without having to become an IT administrator. Creating and running a network security game requires creating VMs, installing and configuring software, and configuring the network. This includes both the "game space" as well as the management space, e.g. scoring system and firewalls that define the rules of the game and what players can do. EDURange is designed to abstract the game configuration in order to highlight the learning goals rather than the system configuration details. These details are captured in machine-readable configuration files that the instructor may modify if desired.

Participants should come away with practical exercises and techniques they could use in their own classrooms. The topic that we will focus on is the interplay between reconnaissance of a network and network defense using a firewall. Participants will learn about the levels of protection that a firewall affords and how to gather information about a network that is protected by a firewall. One of the main challenges with firewall configuration is that the rule set itself has restricted capabilities. A firewall has a limited view of the traffic that is entering and exiting the network. Nevertheless, we can describe the basic structure of the rules and how to protect against some of the standard attacks. We will use iptables on Linux, but we will also discuss Windows Firewall and firewall appliances. The first step is to try to identify and describe the possible ways an attacker can gain access to a resource or information. This has a large analytical component. In order to defend against reconnaissance tools, the participant should understand how traceroute, nmap and ping work. During the exercise, participants will be asked to reconfigure the rules to add services in a safe manner. At the conclusion of this tutorial we will discuss the exercise and how it could be used to develop analytical skills.

In the long term, teaching instructors about security also provides opportunities for our students. A significant cybersecurity workforce will provide a strong pillar for the domestic high-tech industry. The nature of these jobs demands that they remain in the United States for the long term, and they would directly support efforts to introduce practices of information assurance into various parts of the business sector (e.g., the health care and energy industries) in a secure and reliable fashion. By providing access to this information to our students, we are increasing their opportunities to find rewarding careers after graduation. All of the proposers have been teaching cybersecurity at the undergraduate level using interactive exercises.

ACKNOWLEDGMENTS

We are very appreciative of the support from the National Science Foundation through grants TUES-1141341 and TUES-1141314.

REFERENCES

[1] ACM/IEEE-CS Joint Task Force, Computer Science Curricula 2013, 2013, http://ai.stanford.edu/users/sahami/CS2013/, retrieved June 15, 2013.

[2] EDURange, http://blogs.evergreen.edu/edurange/, retrieved June 15, 2013.