CyberCorps Range Management Guide

Introduction

As discussed in the CyberCorps Facilitator’s Guide, the key components of the CyberCorps Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL) include the BetaPort virtual range environment, faculty and/or external expert facilitators, human factor requirements and the CyberCorps Participant’s Guide. Each of these sections provide other higher education institutions considering the learning laboratory experience with a “cookbook” outlining all of the elements of the VCCLL recipe. While the Facilitator’s Guide focuses on the processes involved in recruiting and preparing student participants in cyber security simulation, the management guide section offers advice and suggestions for recruiting and preparing students and other personnel for the equally important work of building and maintaining the range infrastructure, as well as actually conducting the cyber security simulations. Like their counterparts on the front end of these simulations, students and other personnel involved in managing the back-end operations of the cyber security range must be involved in all phases of the planning and execution of cyber security simulations.

Planning and Recruiting

In the University of Southern Maine VCCLL pilot the team primarily responsible for building and maintaining the range consisted of three people: two students and a staff member for supervision. Based upon our experience, the students should ideally have completed courses in networking, web design and programming prior to joining the back-end team. Student academic training should align with the infrastructure of the hosting institution. At USM, the range infrastructure including all network routers, firewalls and host systems is Linux-based. Therefore, it was helpful to recruit students with some background in using or managing Linux systems, especially at the command line, if possible.

In addition to the core team, additional team members must be recruited to assist in various ways in planning and conducting cyber security exercises. These additional personnel will typically participate on a part-time basis and may include faculty members with expertise in cybersecurity and information technology operations, industry experts and students. These additional personnel may need to fill a number of roles including website and software development, planning exercise scenarios and acting as non-player characters (NPCs) during cyber security exercises.

Pre-work

Institutions considering the VCCLL model should consider opportunities for students to enhance their skills in preparation for working in the the range. The work of building and maintaining the cyber security range requires expertise in a number of IT-related areas that may not be covered in many computer science and IT programs. For example, team members will require skills in creating and maintaining virtual computing environments; installing and configuring several types of network devices; installing, configuring and maintaining a wide variety of network
services; creating and deploying a number of websites and applications; and creating and managing user accounts, among others. Depending on each student’s background and experience, significant preparation in networking, web development and system administration may be required before students can constructively contribute to this effort. Institutions may consider alternatives to traditional classroom work, such as boot camps and intensive workshops, which can provide interested students with needed skill-building opportunities and a chance to connect with other “back-room” team members. Those connections are extremely valuable in developing familiarity and trust among backroom team members.

In addition, the task of developing and running cyber security exercises depends on a number of different software tools used to generate both benign and malicious network traffic of various types, depending on the chosen exercise scenarios. Experience shows that while some off-the-shelf software, both open source and commercial, can be used to meet these needs, other tools will likely need to be developed in house. For a description of USM’s approach and experience in this area, see the Scenario Development document.

**The Cyber Exercise Process**

As described in the CyberCorps Facilitator’s Guide, cyber exercises are typically scheduled in two distinct, back-to-back phases: a warm-up day and a game day, followed by a combined faculty, staff and student debriefing after each scenario. Each day-long phase of the exercise process was designed to address key aspects of the virtual cyber experience, as student participants are asked to absorb a great deal of information about the nature of the anticipated scenario experience. It is clear from the VCCLL experience that selected students must be prepared; academically skilled, socially adept and intellectually engaged to gain the most from participation in complex scenarios.

**Warm-Up Day**

The primary objectives of the warm-up day are to help student participants become comfortable in their assigned IT staff roles, develop an effective workflow pattern with their fellow IT staff members, and to get a sense of what a normal level of activity looks like on the BetaPort network. To create a sense of normalcy for student participants, the back-end team members launch a collection of Python scripts to generate a baseline level of benign network traffic simulating the various kinds of activity commonly found on analogous network systems, including routine email, XMPP chat, Web browsing, audio streaming and other kinds traffic. Ensuring that student participants develop a good sense of “base-line” or normal operating traffic is critical to students being able to move beyond normal functionality and understanding network problems (see the Scenario Development section for details). Team members also act as monitors of the BetaPort network to ensure that all nodes are functioning normally and they are positioned to ideally remedy any technical issues that may arise during the simulation.

In addition, several of the back-end team members assume roles as company officials, customers or clients; in these roles, they interact with student participants during simulations via email, chat and telephone. Through these activities, non-player characters (NPCs) help to direct
the flow of the simulation and guide the activities of participants by requesting information about or reporting problems with network resources. The warm-up day gives the back-room students the chance to become more familiar with these character roles and to “practice” interactions with student participants.

**Game Day**

Game day provides a number of unique challenges as the ebb and flow of the day is often determined by the scenario chosen for the day’s event. Back-end team members’ responsibilities on game days involve all the same activities as on warm-up days. Additionally, depending on the scenario chosen for the exercise, team members are also responsible for launching one or more cyber attacks on selected BetaPort systems. Depending on the nature of student participant responses and the selected exercise scenario, NPCs may also become involved in the scenario in various ways. For example, early notice of an attack may be provided through exercise inputs in the form of cell phone calls or other communications from various NPCs to BetaPort company helpdesks to report system outages or other issues related to the simulated cyber attack.

Back-end team members are expected to carefully monitor network status during exercises. In addition to detecting and responding to routine technical issues that inevitably arise, team members may also be required to assist student participants (indirectly and in the context of the exercise scenario) to restore network nodes or services disrupted as a result of participant mistakes. Experience shows that cyber exercise activities are sometimes brought to a standstill as a result of misguided or accidental misconfigurations or overly-aggressive actions that result in lost network access, downed systems or inaccessible or deleted accounts. In such cases, the range management team should consult with NPCs and exercise facilitators to determine the cause an outage, and then to guide exercise participants to a solution so that the exercise can continue. Such disruptions can often provide valuable learning opportunities that can be capitalized on during the post-exercise debriefing.

**Debriefing**

For the VCCLL project, debriefing was not only a reflective learning process for students but also a key, iterative process for the faculty and staff enabling the VCCLL team to adjust scenarios, pre-game and game day activities and processes. Students learn best when they are actively engaged in the process, participate, play a role, and experience not only concrete events, but also transactional events. The role of debriefing, particularly in active, “participation” based activities is an important factor in understanding and increasing the effectiveness of learning. Additionally, the concept of reflection on an event or activity and subsequent analysis is the cornerstone of that experiential learning experience. Led by VCCLL facilitators, student participants were able to share their experiences and reflect both on the active nature of the experience and their making sense of the event in a supportive, respected climate.
Based upon the VCCLL experience we strongly encourage that following each day’s cyber security simulation, back-end participants are brought together to review what took place during the simulation, discuss lessons learned and solicit suggestions for improving future simulations. Specifically, it was very helpful to review and evaluate the effectiveness of the following back-room operations:

- Infrastructure performance and technical issues. These should be listed, described and scheduled for remedy.
- Realism of traffic, and level of traffic activity. Did benign traffic seem realistic to participants? What about the level of activity? Too much, too little? (All scripts used in the VCCLL pilot to generate the Truman Show activity can be configured to adjust the level of traffic.)
- The roles and contributions of NPC’s. What about NPC inputs? Were these realistic and effective? Not all users and administrators provide reasonable or helpful inputs to IT staff, so a bit of confusion might be appropriate. In cases where NPCs were looking to coach participants to a solution, was that coaching effective and helpful?
- Completeness of scenarios. What, if anything, seemed to be missing from the scenario, both in terms of benign traffic and symptoms of the attack(s)?