Cyber Defense Exercise: A Service Provider Model

Jeffrey A. Mattson

Software Engineering Institute, Carnegie Mellon University, 4500 5th Avenue, Pittsburgh, PA 15218
jmattson@cert.org

Abstract. Cyber Defense Exercises (CDX) continue to gain appreciation in the context of information security education. Primarily conducted in academic environments, the call for CDX is beginning to breach that boundary. Existing models are challenged by cost, agility, legality, and scope. This paper presents a model that addresses these challenges through a CDX service provider model.

Keywords: Cyber Defense Exercise, Training Information Assurance Professionals, Information Security Education.

1 Cyber Defense Exercise

Cyber Defense Exercises (CDX) are training events designed to educate participants in the field of information assurance and cyber security. The general concept requires a team to defend a computer network, including the hosts and devices that comprise the network. CDX has grown in popularity since 2001 when the United States Military Academy challenged her sister service academies to an information security competition. Many other universities have developed similar exercises, most often to directly support their information security curriculum. For the past two years, there has been an influx of schools engaging in these exercises through the National Collegiate Cyber Defense Competition [1]. The NCCDC has provided a format and structure that allows schools to compete locally and regionally toward the goal of reaching the annual national competition.

This popularity is driven by the significant impact that the hands-on, real-world training these events provide. The literature on cyber defense exercises consistently describes the enthusiasm of participants for the knowledge gained and lessons learned. An exercise of this sort serves as a natural capstone to a holistic information security education program.

The CERT[1] training program serves the professional community through a traditional educational model to build a knowledge foundation through lecture and demonstration, followed by confidence-building labs and exercises. In this "hear, see, do" structure, students gain not only knowledge, but experience as well.

[1] CERT is the Networked Systems Survivability program at Carnegie Mellon University's Software Engineering Institute. One of its missions focuses on the development and education of best practices for Information Assurance.

1.1 Academic Boundary

The Cyber Defense Exercise Workshop, sponsored by the National Science Foundation in 2004, recommended the CDX stay confined for a time to the university setting [2]. The CDX process could better mature and incorporate into the information security discipline if its focus was initially on the academic exercise. It is clear, however, that some outside of academia are already interested in the training benefits a CDX can provide. All of the Armed Forces branches, as well as the Department of Defense as a whole, are looking for ways to validate the effectiveness of their Information Assurance professionals. The DoD 8570 directive requires personnel in information assurance positions are certified at an appropriate knowledge level [3]. The CDX may be a vehicle by which those goals can be met.

Many other government agencies are following suit. As the government is now implementing legislated requirements for the strengthening of information security processes, they are looking for ways to enhance their training. The Federal Information Security Management Act formalizes a rigorous review of information security processes for all government departments [4]. Included in those processes are mechanisms for workforce education and training.

It is likely that industry will follow. The University of Texas in San Antonio's 2006 CDX networks were defined as typical small business networks as that was a likely future environment for most of the participants [5]. As students who have benefited from this exercise permeate business environments, they may likely bring with them this idea of CDX training.

1.2 Training for Professionals

One of the common complaints of exercise participants, in the case of an early USMA Service Academy CDX, was lack of preparedness in network systems administration. This is explainable as "...the Computer Science Accreditation Board does not emphasize network administration, but rather software creation. Thus, these cadets learned the same lessons that system administrator would also learn by experience "[6]. This reinforces the point that a CDX can provide some experience to those without it; very similar to "on-the-job-training". This experience helps students understand the knowledge they have acquired in more traditional academic settings. However, by regretting their lack of experience, students imply a desire to undertake the exercise with the requisite experience. Consider then the effect of a CDX on IA professionals, those with varying degrees of experience already in hand. The focus shifts from gaining knowledge to demonstrating knowledge. The exercise can serve primarily as a continuing education, skills validation or a team-building exercise, rather than grounds for knowledge synthesis.

2 CDX Features

The Cyber Defense Exercise Workgroup defined four types of CDX popularly implemented: the organized CDX competition, the continuous internal exercise, the re-

gional capture-the-flag exercise, and the class-integrated exercise. Of these four, the first is the best candidate for the expansion from academia to industry. If the focus of the exercise shifts from learning to validation, integration with a specific curriculum is no longer necessary. The continuous internal exercise has a bit of a game feel to it, and lacks a discrete ending point and performance review. The capture-the-flag model also lacks the structure and organization to effectively evaluate a team on cyber defense. The organized CDX offers the key features necessary for an evaluation exercise.

2.1 Defense

The participants are focused on network defense only. The legality of computer attacks makes any offensive effort of an exercise questionable. Especially in a validation of cyber defense skills, there seems to be little need for the participants to employ any offensive tactics. This scenario uses third-party IA professionals to objectively test the defenses of each team. As such, participants are not evaluated on attacks, but only on defense.

2.2 Administration

Exercise participants can be completely responsible for the administration of their networks. Because the exercise duration can be well defined, and generally short, the students are generally able to administer the networks from setup to tear-down. This applies to most event structures: both where networks are preconfigured and provided and those where participants must build and design a network of their choice.

2.3 Isolation

It is imperative that a CDX is conducted on an isolated network. Unfortunately, for a validation exercise this usually means some loss of realism. It would be ideal to evaluate participants' skills on the very network they maintain; however, the risks associated are generally too high. Any exercise incident, whether malicious or not, could end up affecting real-world events, so separate, isolated networks are highly encouraged. The level of realism the "range" network provides stems from availability of the organization's resources. In many cases it seems possible to construct a reasonably similar training network.

2.4 Competition

In the academic setting, much of the participant motivation is generated through competition. While competition may have less influence in a corporate or government evaluation environment, it can still play a part. Organization's that are large enough may submit several different teams to a CDX, and such intramural competition may be leveraged to strengthen enthusiasm. The primary motivation, however, comes

from the desire of the participant to demonstrate his skill-set to his employer. As managers work to maintain a skilled workforce, often in need of some reportable measure of certification or compliance, they may find value in CDX and request employees to validate or assess their skills.

3 CDX Enhancements

To support the CDX at a much wider scope than currently employed, the CDX model can be enhanced and streamlined. It is foreseeable that IT training and education companies may add the CDX capability to their suite of offerings. Such a move would provide a significant service to those desiring a CDX. The difficulty and hassle of occasionally setting up and coordinating an exercise would vanish for an organization that was focused on delivering CDX services. As commercial opportunity grows for the management of CDX, we anticipate streamlined governance and exercise management, reduced costs, and more effective communication.

3.1 Virtualization

Constructing a CDX environment based on virtualization provides a significant improvement in scalability, agility, and isolation. Commercial products that provide the ability to create and run virtual machines have matured considerably in recent years. This provides a simple means to maximize use of the physical resources on hand. Thus, the number of physical hosts necessary to produce the exercise network is easily four times fewer than virtual machines.

A virtual environment is also one that maximizes agility. The ability to change directions quickly to meet new needs is fostered by virtualization products, especially those with snapshot capabilities. With a collection of base virtual hard disks, it can become a push-button operation to add new machines to the network or to revert all machines back to a known starting state. Customers of a CDX could potentially build their exercise network topology by just selecting a few menu options.

Further, virtualization generally provides built-in network isolation. The entire exercise network, including Red Team hosts, can be separated from other networks. Access to the exercise network could be through a portal, allowing participants to enter the lab environment from anywhere with network connectivity. This portal can provide participants with a remote session on a virtual host attached to the virtual network. With only the remote session desktop image being allowed out of the exercise network, returning to the participant's computer, the threat of a malicious event breaching the wall of isolation is mitigated. This concept allows for the formation of virtual teams -- participants who are not physically co-located but can contribute to the same mission from anywhere around the world.

3.2 Cost Reduction

While virtualization can ease the cost burden of procurement and maintenance, centralization of CDX services can also mitigate personnel costs. The service provider can fulfill multiple roles in the exercise conduct, such as exercise setup and management, referee, or White Team, and even the Red Team role. While it could be easy enough to provide a third party Red Team with virtual hosts in attack position, it is also feasible for the exercise controller to have at his disposal a set of scripted, push-button attacks. At any rate, the service provider model can significantly free the educators or managers time for other work.

3.3 Communication and Feedback

With the ability to handle virtual teams that connect to the exercise network from dispersed locations, providing communication services becomes mandatory. The exercise entry portal can be equipped to allow for intra-team and white team communication. Bandwidth options could allow either video, voice, or text chats, so that the team could assemble in a virtual room. Further, the portal can provide a logging mechanism to capture event information during the exercise. Because the whole of the network resides in the service provider's domain, they can capture real-time logs of exercise events, to include Red Team actions. This translates into rapid information collation and a support for a timely after-action review. In the traditional CDX, it is not uncommon for the assessment to follow the exercise by several weeks. Shortening this delay should increase the impact of any lessons learned because they would be offered much closer to the action.

3.4 Uniformity

To be effective as an assessment device or measuring tool, a CDX needs to provide a certain amount of uniformity across instantiations. Not only is it important for competition that all teams are on a level playing field, but it is just as necessary, and perhaps more challenging, to provide a similar exercise scenario to different teams. Currently this is done by conducting simultaneous exercises so that attackers and referees can inject events into the scenario uniformly to all teams. Then the question remains of uniformity from year to year, or even event to event.

One way to address this is through a formally, but flexibly, scripting the scenario. Providing detailed objectives, and defining various levels of success, allows results from different exercises to be compared with a higher degree of confidence. To borrow from the military's vocabulary, each event expected during the scenario can be broken into Tasks, Conditions, and Standards that allows for fine-grained assessments.

3.5 Other considerations

There are several issues yet to work out in a CDX service provider model as described. The issue of network devices affects the streamlined nature of a completely virtualized environment. Any use of physical devices would impact the agility and scalability with which a provider can offer services. While having physical devices may be essential to some environments, there are several in which exercise objectives could still be met using virtual replacements.

Also, it would be necessary to provide some means of downloading software or importing non-standard tools into an isolated exercise network. Without access to the physical machines, participants would need to coordinate with the service providers for this capability.

4 Conclusion

The CERT Practices, Development, and Training team has focused on improving Information Assurance Training for many years. The training concept used is reflected in the slogan "Knowledge in Depth for Defense in Depth". The KD3 program builds on a traditional education foundation of instructor led classes with lecture, demonstration, and hands-on lab exercises. Following individual training, teams need be trained on both network assessment and cyber defense. Because this team training is increasingly sought after and difficult to reproduce, it is an excellent candidate for implementation under a CDX service provider model. To fulfill the growing call for this effective, exciting training, the future of CDX development should aim in this direction.

References

1. National Collegiate Cyber Defense Competition. *http://nationalccdc.org/history.html.*
2. Lance J. Hoffman, Tim Rosenberg, Ronald Dodge, and Daniel Ragsdale, "Exploring a National Cybersecurity Exercise for Universities," *IEEE Security & Privacy*, vol. 3, no. 5, September/October 2005, pp. 27-33.
3. U.S. Department of Defense Directive 8570, *Information Assurance Training, Certification, and Workforce Management*, August 15, 2004.
4. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
5. Art Conklin, "Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course", in *Proceedings of the 39th Hawaii International Conference on System Sciences*, 2006.
6. Donald Welch, Daniel Ragsdale, and Wayne Schepens, "Training for Information Assurance", *IEEE Computer*, vol. 35, no. 4, March 2002, pp. 30-37.