Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015

Jelena Mirkovic
USC/ISI

Aimee Tabor
University of California, Berkeley

Simon Woo
USC/ISI

Portia Pusey
National CyberWatch Center

Abstract

Cybersecurity competitions are popular tools for attracting students to cybersecurity field. Yet, many competitions require extensive preparation, strong coding skills and solid background knowledge, not just in security, but also in system administration, networking and operating systems. As such, competitions may discourage novices that lack in one of these required areas. In this paper we discuss our experience in using Class Capture-the-Flag Exercises (CCTFs) to bridge this gap in classes, and in 2015 ACM Richard Tapia Security workshop. We recount lessons learned and map a way forward, towards collaborative, more structured cybersecurity competitions that better support and engage novices, and offer a positive learning experience to all.

1 Motivation

Cybersecurity competitions are fun and engaging, and seem like a fitting tool to attract students towards a specialization and a career in cybersecurity. Many such competitions are organized nationally, with varied goals and levels of difficulty. Some examples are DefCON [10], iCTF [17] and CCDC [3]. But, while competitions are fun, they are also humbling to many teams that do not win. Many competitions draw teams from varied backgrounds, some with players who have been hacking for years. Being competitive at such an event requires extensive preparation, strong coding skills and solid background knowledge, not just in security, but also in system administration, networking and operating systems. As such, competitions may discourage novices that lack these needed skills [15]. These participants may find themselves so out of their depth, losing in their first round or not being able to keep up with a much better prepared team, to forsake cybersecurity altogether.

In this paper we discuss how we could design cybersecurity competitions that offer a positive learning experience for novices. Ideally, such competitions would focus primarily on learning, team-building and awareness-building. The secondary goal should be to promote an adversarial mind-set. Further, such competitions should require short preparation time and should compensate for varied background and skill level of participants. Finally, individual skill levels should be considered when creating teams, so team capabilities are balanced and each team has a chance to win.

With a desire to gently introduce novices to cybersecurity competitions, Mirkovic and Peterson designed Class Capture the Flag (CCTF) exercises [12]. These are small-scoped, hands-on exercises in defense and offense, designed for class use. CCTFs have been implemented in cybersecurity classes at University of Southern California, and are recently publicly released via DeterLab testbed [6]. CCTFs have modest preparation and execution time – a few weeks of preparation and a few hours of competition. Student competitors organize in teams and engage in offense-defense scenarios, which pit them against teams of similar skills and background. This evens the playing field, giving everyone a chance to win. Further, each team plays both the defensive and the offensive role. This helps the participants practice and acquire the adversarial mindset needed for a career in cybersecurity.

After each CCTF, the teacher leads an in-class post-mortem analysis of the event. This process provides the critical feedback, which should enable students to recognize what they did right, and to identify areas that require additional practice. Moreover, teams that did well in the CCTF are given the opportunity to teach other teams their successful strategies during the post-mortem. An overall goal of CCTFs is to expose students to adversarial scenarios that are a part of practicing cybersecurity, in a way that promotes learning. Ideally, a teacher would run several CCTFs within one class offering, enabling students to progress in their learning and apply lessons learned from one event to the next one. CCTFs are also conceived as a path to prepare for more rigorous and demanding cybersecurity competitions.

CCTFs and teacher experience from using CCTFs in class are described in publication [12]. In this paper we describe how we used the Resilient Server CCTF, which includes a denial-of-service scenario, in a new setting: at the Security workshop at the 2015 ACM Richard Tapia conference. Our goal was to engage 18 self-selected students, coming from institutions across the United States, in a cybersecurity exercise in order to expose them to the fundamentals of network security. These students had very different background and preparation than our regular CCTF participants. Most students had no formal security coursework or training, and none have completed preparation prior to the exercise. We recount how the exercise unfolded and what we learned from it about tailoring cybersecurity competitions for novices. We also evaluate student learning in this setting using a pre- and post-exercise survey.

2 Novices and Competitions

Many cybersecurity competitions are organized nationally and internationally, e.g., Cyber Patriot [1], CCDC[3], iCTF [17]. While their goals, difficulty and target populations differ, most competitions focus on hacking – finding and exploiting vulnerabilities in a target system. Most frequent three types of competitions are described below:

- **Offense**: Teams of participants race to detect and exploit vulnerabilities in a given target platform in a limited time.
- **Defense**: Teams of participants defend their system against a dedicated Red team, which performs offense.
- **War Game**: Each team of participants has its own system to protect. Each team can attack the system of any other team.

2.1 Challenges for Novices

Cybersecurity offense and defense require a lot of attention to detail. They often have several steps that must be executed in the right order and with the right parameters to get a desired result. Many attacks are environment-sensitive, they may work in one environment (e.g., one operating system or a network with a given setup) and fail in another one. On the other hand, there is frequently more than one way to achieve a desired goal, e.g. to break into a machine, hijack its traffic, or detect and mitigate a given attack. This mix of importance of details (the right steps, the right environment) and breadth of possibilities (many possible attacks and defenses) is what makes cybersecurity competitions both interesting and challenging.

Competition participants also need very strong coding skills (preferably in some scripting language like Perl or Python), good knowledge of Linux or Windows operating system and strong networking skills. Without these prerequisites, many participants cannot meaningfully contribute to their team's effort, even if they have good knowledge of security concepts from reading or lectures.

The situation is particularly dismal for novices that may lack both the needed background in cybersecurity (necessary to understand details and possibilities of attack/defense) and strong coding skills. Thus an early exposure to cybersecurity competitions may discourage many novices from further involvement in the cybersecurity field – an opposite goal from the one we would like to achieve [15]! Still, games and competitions are fun and resonate with young people, and thus could be a good way to build awareness and attract interest. The challenge then lies in keeping the playful and competitive spirit, but adjusting the structure and difficulty of competitions to make them a good recruitment and engagement tool for novices.

3 Class Capture-The-Flag Exercises

Class Capture-the-Flag exercises (CCTFs) were created by Dr Mirkovic and Dr Peterson, at the University of Southern California. They are designed for students who take an introductory cybersecurity class. The goal is to introduce students to the adversarial mind-set that occurs in realistic cybersecurity scenarios, and to help them build practical skills for a future career in cybersecurity. Further, our vision for CCTFs was that multiple instances would be played during one class offering, enabling students to identify areas for improvement in one instance, and hone them until the next one. CCTFs focus on learning more than on competition. While teams prepare in isolation from other teams, they are encouraged to discuss their challenges during a competition. The teacher may instruct a team that does particularly well on a task to share their ideas with other teams. After a CCTF, the teacher leads a post-mortem discussion where each team reports on the strategy and tools they deployed, how these had worked out and what the team had learned. Our intent was that this discussion would help under-performing teams and students identify areas for improvement, and offer ideas for winning strategies.

When compared with traditional competitions, CCTFs differ from them in the following design choices: (1) Shorter preparation (a few weeks) and run time (a few hours), which facilitates scheduling multiple CCTFs during one class offering, (2) Focus on different cybersecurity topics, not just hacking. Currently CCTFs exist on cryptography, intrusions, denial-of-service and DNS security. (3) Designed for learners, not experts. CCTFs assume preliminary knowledge of cybersecurity, networking and operating systems, such as could be obtained through self-study of links provided in a CCTF, or through an introductory cybersecurity class. (4) CCTFs engage participants both in offense and defense, while traditional competitions only engage them in one of these modes.

CCTFs are executed on the DeterLab testbed [16], a large, public and free-for-use cybersecurity testbed hosted by USC/ISI and UC Berkeley. The testbed is accessible remotely via SSH and Web browser, which facilitates participation by remote teams.

In publication [12] we have informally reported on the lessons learned from running CCTFs in an undergraduate class at University of Southern California in 2012 and 2013. In this paper we recount our experience of using one CCTF at the Security workshop at 2015 ACM Richard Tapia conference, organized by the TRUST center to attract novices to cybersecurity. We further report on the instruments we used to evaluate learning during this competition, and on promising results.

4 Security Workshop at ACM Richard Tapia Conference

The ACM Richard Tapia Conferences bring together undergraduate and graduate students, faculty, researchers and professionals in computing to celebrate diversity and create communities that support it. During registration, participants have the opportunity to opt in to several activities that happen on the Saturday after the conference. Activities include university tours, industry visits, and workshops in robotics, security and other topics that vary each year. Student participants come from a wide variety of two-year, four-year, and graduate universities. There are no prerequisites to attend. However, participants are required to fill in a web form when registering for workshops, stating their familiarity with programming languages, security topics, and any specialized tools that will be used during the workshops.

The TRUST Center (https://www.truststc.org/) has hosted the Security workshop at the ACM Richard Tapia conference for the past two years. Prior to the first TRUST-sponsored Security workshop, a theoretical Capture-the-Flag exercise was offered to the Tapia attendees. It was done in a lecture-group format, where participants brainstormed an adversarial scenario. The TRUST Center endeavored to continue the workshop, but to transform the CTF exercise to be hands-on, to boost the participant engagement.

With traditional CTF exercises, participants form groups themselves and have anywhere from weeks to months to prepare for the exercise. Many schools form student teams for traditional CTF competitions. During preparation time these student teams are often supported by an instructor or group/team leader with security and CTF experience [13]. During class CTFs (CCTFs), the class instructor creates the groups and assigns tasks. Preparation time is shorter than for a regular CTF exercise (a few weeks versus a few months) and the tasks are easier and more structured. For these reasons we have decided to use a CCTF for the Security workshop at the 2015 ACM Richard Tapia conference. Our hope was that the short preparation time, better structure and lower task difficulty would be better suited for novices.

4.1 Resilient Server CCTF

We chose to use the Resilient Server CCTF [7] for the 2015 Security workshop. This CCTF focuses on distributed denial-of-service (DDoS) attack and defense. During a denial-of-service attack, the attacker floods a server with high volume of traffic, from multiple machines, which overwhelms the server and denies service to its legitimate clients. Any traffic can serve this purpose as long as it is high volume. This simplicity of the attack aligns it well with the diverse backgrounds and the dearth of operating system and networking knowledge in the workshop participant population. It also opens many opportunities for varied attack and defense strategies.

Figure 1 shows the topology used for this CCTF. All nodes are running Ubuntu Linux. Participants divided into defenders (Blue group) and attackers (Red group). The Blue group is given access to the server node, which is running an Apache Web server, and the gateway node. The Red group is given access to two out of three client machines and can use them to flood the link between the gateway and the server. The remaining client machine was acting as legitimate client, and no group had access to it. All client machines were automated to continuously send Web requests to the server, at the rate of one request per second. Links between the clients and the router, and the link between the gateway and the server had 100 Mbps bandwidth. The link between the gateway and the router had 1 Gbps. This setup allowed the malicious clients to flood the link between the gateway and the server by sending high-volume traffic from two client machines.

The Red group's task was to make the server unable to serve its legitimate client through denial of service. They could choose which resource to flood (the server or the link between the server and the gateway), the type of traffic for flooding, and the dynamics (continuous or sporadic). The Blue group's task was to defend from the attacks, e.g., through diagnosis, profiling and filtering, and to ensure that the legitimate client's requests get served. The Blue group did not know the identity of the legitimate client, but could attempt to infer it through traffic monitoring. The Red group could use IP spoofing in its attacks to mask the identities of the malicious clients. Due to reduced preparation time, we have provided Red group with two tools that can create various flooding attacks: Flooder [2] and Slowloris [4]. The Flooder tool builds raw packets, whose headers, length and rate can be customized from the command line. This tool can be used to flood the link between the gateway and the server. The Slowloris tool opens multiple connections with the server and keeps them open by continuously sending HTML headers. This creates denial of service at the server, since no sockets are left for the legitimate client's use.

The exercise was scored based on the legitimate client's experience. The traffic trace was collected at the legitimate client's machine and mined to calculate the time needed to complete each Web request. Replies that took less than 0.5 seconds brought a point to the Blue group. Otherwise, the Red group scored a point. The score for each team was the sum of the scores for its Blue and Red groups.

This exercise teaches students how to create and defend from various denial of service attacks. It also trains them in using various tools and platforms, like the Linux platform, the Slowloris tool, the tcpdump tool, the iptables tool, etc. Finally, it teaches the importance of monitoring and situational awareness, as well as teamwork.

4.2 Pre-exercise

The setting of the 2015 Security workshop created a set of unique challenges that necessitated some modifications in CCTF format. Participants attend the workshop for about six hours, they have not met before, many participants are from schools where security is not taught (or is taught later in the program), and they have varying skill levels and abilities. This did not fit the CCTF participant model, which assumes preliminary background knowledge in cybersecurity, networking and operating systems. It was decided that workshop participants could obtain this knowledge through self-study.

The participants were given access to DeterLab one week prior to the Security workshop, and provided with materials about the competition and the recommended software. These materials included some background slides on DDoS, manual pages for Flooder and Slowloris tools, and the instructions for competition (list of tasks, rules of engagement, etc.).

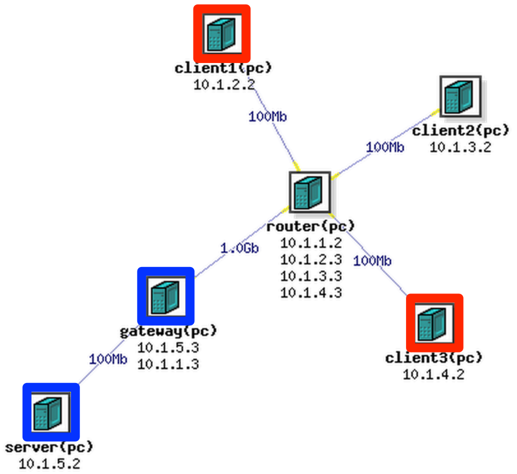

Figure 1: Resilient server CCTF topology

Further, CCTF participant model assumes at least two weeks of preparation time, with teacher guidance, while workshop participants had only one week of self-study. To compensate for this, the participants were provided with an in-person, fifty minute introduction to Linux and DeterLab prior to the workshop, to familiarize them with the interface and configuration of the competition. This mandatory birds-of-a-feather (BoF) session, "Exploring Cyber-security experimentation with Linux and DeterLab," was conducted the day before the competition. Participants learned about the basics of DeterLab testbed, and preliminary Linux commands needed to access and configure the machines during the competition. Additionally, participants were introduced to the traffic analysis tool `tcpdump` [5], which could be used by the Blue group to monitor network traffic.

4.3 During exercise

The 2015 Security workshop, "Exploring Distributed Denial of Service (DDoS)," activity was held on the conference Saturday, from 8:00 am to 5:00 pm, with a break for lunch. Particiipants were divided into three teams – Team 1, Team 2 and Team 3 – and an experiment with the topology shown in Figure 1 was allocated for each team on the DeterLab testbed. Thus there were three competitions running in parallel during the workshop. Each team then sub-divided into the Blue and the Red group. The Blue group had to protect their own team's server, while the Red group was attacking the server of one other team. Figure 2 illustrates this organization of the competition and the access of teams to machines, e.g., the Blue group in Team 1 was protecting its own server, while the Red

Factor addressed	Adjustment	Outcome
Short preparation time	Flooder and Slowloris tools provided	Helped by introducing structure.
Short preparation time	Mandatory BoF with Deterlab and Linux basics	Helped by instructional scaffolding.
Varied skill level	Balanced teams	Helped somewhat. Balancing was done based on initial sign-up data, but fewer participants showed up at the workshop. This necessitated re-balancing of teams half-way through the workshop.
No background knowledge	Background materials	Helped somewhat. Participants did not carefully nor completely read through the materials prior to the workshop.
No background knowledge	Mentors with each team	Helped by instructional scaffolding.

Table 1: Adjustments applied to Resilient CCTF, to make it suitable for novices at the workshop

group in Team 1 was attacking the server of Team 2.

To compensate for varied skill level of participants we have conducted a survey, which asked participants to self-assess their networking, Linux and cybersecurity skills. We used these ratings to form balanced teams for the workshop. To further address shortened preparation time and lack of background knowledge, compared to the CCTF participant model, we have paired each participant team with 1–2 mentors, who had prior cybersecurity experience. These mentors were helping the team understand and conduct the tasks during the competition.

Table 1 summarizes all the adjustments we introduced to the Resilient CCTF to make it suitable for novices at 2015 Security workshop, and the outcomes of these adjustments.

5 Post-exercise

Cybersecurity competitions continue to grow in popularity, partially as a result of their value to employers. Anecdotal evidence supports these three benefits of cybersecurity competitions to government and private industry:

- Provide evidence of professional competence in operational security
- Demonstrate mission-critical performance under pressure
- Assess and benchmark competitors [11]

Our work seeks to explore additional outcomes of cybersecurity competitions. Therefore, an external evaluator was contracted to verify, document, and quantify outcomes of the 2015 Security workshop activities and to make recommendations for future such events. Most importantly, the evaluator administered instruments to examine whether the 2015 Security workshop achieved the following objectives:

1. Engage participants in cybersecurity
2. Improve participants' mastery of skills taught and practiced during the event

To measure if these goals were achieved, the evaluator administered a pre and post workshop quantitative survey to determine participant self-reported change in engagement and self-efficacy regarding skills practiced during the competition.

A modified UTRECHT-9 was used to determine work engagement. The UTRECH-9 has been shown to be a very valid and reliable measure of work engagement independent of gender, age, occupation and nationality. Shaufeli et al. have noted that, "Work engagement is defined as a positive, fulfilling work-related state of mind that is characterized by vigor dedication and absorption" [14]. Using a Likert-type scale respondents reported on the three characteristics that contributed to a single engagement score:

- **Vigor**: high levels of energy and metal resilience, willingness to invest effort into ones' work and persistence even in the face of difficulties
- **Dedication**: involved sense of significance, enthusiasm, inspiration, pride and challenge
- **Absorption**: fully concentrated and happy

There were three questions for each of the characteristics measured. For example the following is a question that measures dedication: "Defending and/or attacking computer networks inspires me". Workshop participants were able to respond using a scale that ranged from zero to six. A rating of zero indicated that they never felt inspired, a rating of six indicated the participant always felt that way (every day).

Engagement is strongly related to professional efficacy. Self-efficacy is an indication of a person's belief

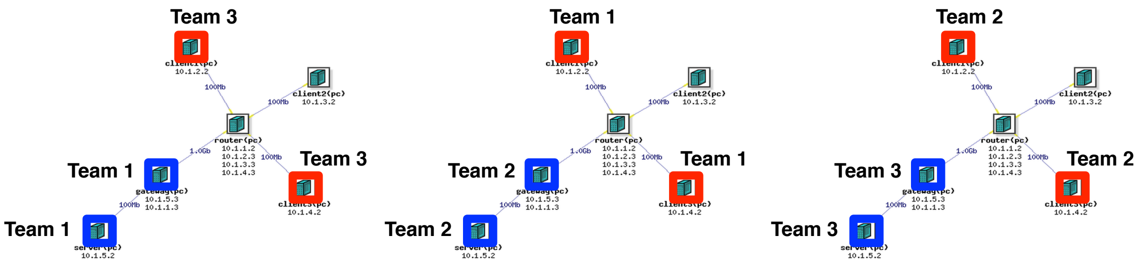

Figure 2: Pairing of participants into teams, and subdivision into Blue and Red groups

that they can accomplish a specific task [8, 9]. However, longitudinal research would need to be done to understand whether self-efficacy might be considered a consequence or an antecedent of engagement rather than a constituting element. The construct of our survey permitted a pre and post measurement of the learning objectives for the event. Each self-efficacy question was composed as follows: "How confident are you that you can successfully <*learning objective*>?".

Additionally, the participants were asked open-ended questions in the survey about their experience and suggestions for future events.

5.1 Evaluation Results

Five respondents among the eight participants who completed the post-event survey also completed the pre-event survey, and we report on these matched-pairs results. While the replies showed an increase in engagement, there were too few matched pairs to report detailed statistics. Similarly, the pre-post measure of self-efficacy shows a trend towards improved skills and higher confidence in using the tools. We show these results in Figure 3.

Analysis of the qualitative data suggested that the participants appreciated having the mentors. The participants said they felt the mentors were patient, helpful, and knowledgeable, and provided individualized attention to struggling participants so that the team could move forward together onto the next tasks. The participants also appreciated the hands-on aspect of the exercise and the fact that they got to work with real tools in an authentic environment. In terms of stated goals for the project, the participants felt that they:

- Were introduced to practical tools for attacking and defending from DDoS attacks,

- Were provided a foundation for tools which will enable them to continue to practice and learn in the future,

- Had gained/improved knowledge of cybersecurity,

- Had gained/improved knowledge of network monitoring,

- Had gained/improved knowledge of the DeterLab system

Furthermore, the participants stated that they were excited to learn packet motoring and learn how to observe the data flows in the network.

6 Discussion

Our experience with 2015 Security workshop has emphasized to us the need to adjust the difficulty and the structure of cybersecurity competitions to better engage novices. We outline below some areas and ideas for improvement:

Balancing teams by skills and seniority. Participant teams should be composed to balance experience and knowledge. We attempted to create balanced teams based on self-rating of participant skills by those that signed up for the workshop. But our attempt was hampered because a smaller number of participants showed up on the day of the event. We needed to re-balance the teams half-way through the exercise. Further, it was evident that the mixture of students in teams from freshmen to graduate presented challenges. Freshmen had a harder time than their older class peers to work efficiently in teams. Creating balanced teams across seniority levels helps address this issue.

Advance collection of demographic and competency information. At the sign-up time, participants were asked to report their knowledge and skills related to topics such as Linux operating system, network protocols, packet analyzers etc. During the exercise we found that this self-reported data was not accurate. Setting up teams based on this information led to one team being much stronger than the other two. We recommend asking more specific questions about the participant knowledge

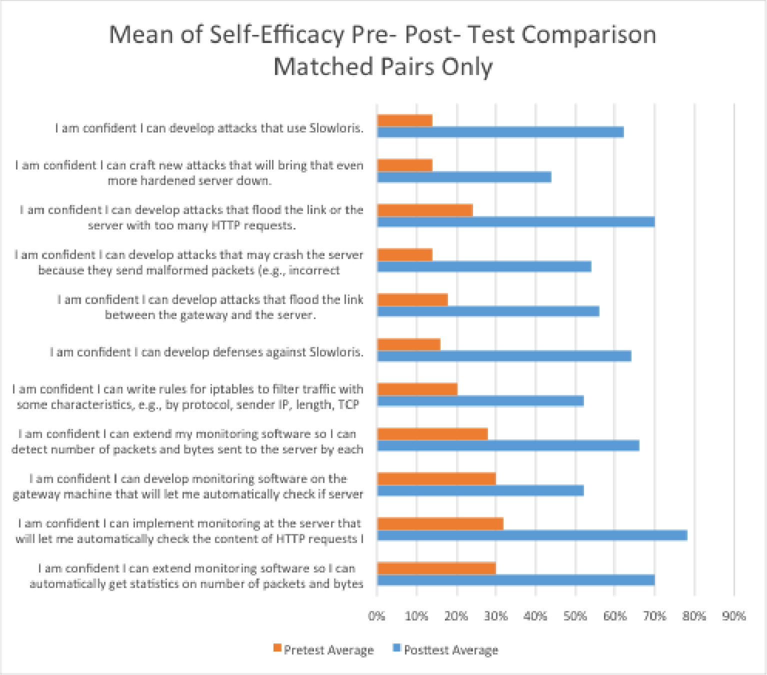

Figure 3: Evaluation results

and skills, or conducting a short quiz-type assessment prior to the event.

Team building. Two out of our three teams had communication problems and did not function effectively together. We recommend providing ice-breaker activities prior to competitions, to create familiarity between team members and to build team spirit.

Event logistics. Communication with the participants was a challenge. Although preparation materials were available a week ahead of the event, and the birds-of-a-feather session attempted to orient participants, many arrived at the event unsure of what was expected of them, or unaware of what the exercise would entail. In post-event surveys, participants requested more exact and specific communication about the schedule and the event pre-requisites. To meet the needs of participants who may be scheduled for the competition at the last minute, and those who did not come to the event prepared, we recommend developing a plan that could bring participants up to speed quickly. Further, the pre-post was only completed by half of the participants. We recommend finding additional incentives for participants to respond to surveys, such as gift cards, to enable better data collection for evaluation.

Additional scaffolding. In post-surveys, participants suggested additional tools that would have been helpful to them in the exercise. They appreciated the oral and PowerPoint description of the structure, rules, and procedures of the activity right at the start of the day to contextualize the learning for them. They additionally wanted white boards, paper on easels, and/or cheat sheets of common commands. Participants found their mentors helpful, but also felt that they needed a way to hold the knowledge in the room, and share what they were learning with the rest of their team. Ability of novices to self-learn was also low. Participants suggested that self-learning should be complemented with activities where mentors model and discuss the required skills and processes.

Changing up the structure. Security competitions assume a lengthy preparation phase, and focus on teams pitting up their skills and knowledge against each other. However, for novice engagement, we need a structure that assumes no preparation and emphasizes collaboration, learning and team building rather than competition. To achieve this in future similar events we plan to evolve CCTFs into "Novice Security Games". In these games, teams would have similar tasks as in CCTFs, but would be offered a series of possible, pre-defined "moves", consisting of tools and input parameters that can either launch attacks, offer situational awareness information or engage a defense. Teams would then focus on selecting moves and understanding their effect on their team's score. This structure would abstract many low-level details that relate to operating system, networking and cybersecurity background, while retaining the spirit of the competition and teaching participants some cybersecurity basics. To emphasize collaboration, learning and team building, frequent briefings and brainstorming sessions could be built throughout the event, both within each team and between teams. These would help bring participants together and share the knowledge. Additionally, some ideas and strategies that emerge in these discussions and are particularly useful could be written down on a whiteboard or an easel, and thus captured for everyone in the room.

7 Conclusions

Cybersecurity competitions seem like a promising tool to boost engagement and attract novices to cybersecurity field. Yet, the structure and difficulty of current competitions may also scare away novices. In this paper we have recounted our experiences with conducting a class capture-the-flag (CCTF) competition at the 2015 ACM Richard Tapia Security workshop, organized by the TRUST center. While our evaluation of the event showed learning and engagement among participants, we have also learned about the organizational and cognitive challenges of conducting competitions with novice populations. We have sketched some ideas that may address these challenges and look forward to testing them in the upcoming events.

8 Acknowledgments

This work was supported by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422). The CCTFs were supported by the National Science Foundation (NSF award number SaTC-1224035). The DeterLab testbed is supported by the Department of Homeland Security (DHS grant number N66001-10-C-2018). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation nor the Department of Homeland Security.

References

[1] CyberPatriot – The National Youth Cyber Education Program. http://www.uscyberpatriot.org/.

[2] Flooder tool man page. http://www.isi.edu/~mirkovic/tapia/flooder.html.

[3] National Collegiate Cyber Defense Competition. http://www.nationalccdc.org/.

[4] Slowloris attack. http://en.wikipedia.org/wiki/Slowloris_(software).

[5] Tcpdump and Libpcap. http://www.tcpdump.org/.

[6] The Deterlab Testbed, Public Access to Shared Materials. https://www.isi.deterlab.net/sharedpublic.php.

[7] The Deterlab Testbed, Resilient Server CCTF. https://www.isi.deterlab.net/file.php?file=/share/shared/ResilientserverCCTF.

[8] BANDURA, A. *Self-efficacy: The exercise of control.* Worth Publishers, 1997.

[9] BANDURA, A. Guide for constructing self-efficacy scales. *Self-efficacy beliefs of adolescents* (2006), 307–337.

[10] INC., D. C. C. DEFCON. http://www.defcon.org.

[11] MANSON, D., AND PIKE, R. The Case For Depth In Cybersecurity Education. *ACM Inroads 5*, 1 (Mar. 2014), 47–52.

[12] MIRKOVIC, J., AND PETERSON, P. A. H. Class Capture-the-Flag Exercises. In *Proceedings of the USENIX Summit on Gaming, Games and Gamification in Security Education* (2014).

[13] PUSEY, P., O'BRIEN, C., AND LIGHTNER, L. Preparing for the Collegiate Cyber Defense Competition (CCDC): A Guide for New Teams and Recommendations for Experienced Players. *National CyberWatch Center Press* (2015).

[14] SCHAUFELI, W., SALANOVA, M., GONZALEZ-ROMA, V., AND BAKKER, A. B. The measurement of engagement and burnout: A two sample confirmatory factor analytic approach. *The Journal of Happiness Studies* (2002), 71–92.

[15] TOBEY, D. H., PUSEY, P., AND BURLEY, D. L. Engaging Learners in Cybersecurity Careers: Lessons from the Launch of the National Cyber League. *ACM Inroads 5*, 1 (Mar. 2014), 53–56.

[16] USC/ISI, AND BERKELEY, U. DeterLab testbed. http://www.isi.edu/deter.

[17] VIGNA, G. The UCSB iCTF. http://ictf.cs.ucsb.edu/index.php.