Teaching Cyber Security through Competition

An Experience Report about a Participatory Training Workshop

Akbar Siami Namin
Department of Computer Science
Texas Tech University
Lubbock, TX, USA
akbar.namin@ttu.edu

Zenaida Aguirre-Muñoz
College of Education
Texas Tech University
Lubbock, TX, USA
z.aguirre@ttu.edu

Keith S. Jones
Department of Psychological Sciences
Texas Tech University
Lubbock, TX, USA
keith.s.jones@ttu.edu

***Abstract*—Training workshops and professional meetings are important tools for capacity building and professional development. These social events provide professionals and educators a platform where they can discuss and exchange constructive ideas, and receive feedback. In particular, competition-based training workshops where participants compete on solving similar and common challenging problems are effective tools for stimulating students' learning and aspirations. This paper reports the results of a two-day training workshop where memory and disk forensics were taught using a competition-based security educational tool. The workshop included training sessions for professionals, educators, and students to learn features of Tracer FIRE, a competition-based digital forensics and assessment tool, developed by Sandia National Laboratories. The results indicate that competition-based training can be very effective in stimulating students' motivation to learn. However, extra caution should be taken into account when delivering these types of training workshops.**

Keywords-component; cyber security, digital forenciscs, partcipatory training workshop, competition-based learning, assessment

I. INTRODUCTION

Simulation and competition-based exercises are viable and effective tools for training students about fundamental and advanced attacking (red team) and defending (blue team) techniques. The collaborative environment embraced by competition-based learning enables students as cyber defenders, i.e., the blue team, to create and build better tactical strategies against cyber attackers, i.e., the red team. It has been reported that students would grasp the scientific concepts and tactical strategies better when formed into two groups of red and blue teams where the team members of one group acts as attackers threatening the assets, infrastructure, and cyber system of the other team [16, 17, 18]. More specifically, these attacks and defense strategies are often framed in the form of activities conducted by red and blue teams, where the red team intends to exploit some vulnerabilities of the infrastructure operated by the blue team.

An effective simulation-based training requires carefully designing and developing structured instructional materials and modules, each focusing on teaching certain cohesive aspects of the underlying security concept with the goal of revitalizing certain desired skillsets. *There are two major problems associated with the existing competition-based educational tools for teaching cyber security*:

The *first* major problem is that the existing tools often overlook the vital impact of behavioral, social, or even ethnographical aspects of cyber security scenarios when designing attackers/defenders educational and simulation tools. The behavioral models are rooted in the fundamental principle that regards an individual's cognition and mindset as playing an influential role in development of behavioral responses and actions to life responses taken in real world events [19]. Under the cybersecurity context, there are several situations that require understanding behavioral and cognitive aspects of both attackers and defenders in order to analyze the attack's intention or predict the attacker's next move. Similarly, it is important to take the attackers' skillsets into account and guide defenders to be well-prepared when confronting such cyber attacks. For example a well-prepared defender could respond to a cyber attack incident in an agile manner and recover from disaster rapidly. A well-developed training module based on behavioral task analysis can prepare the cybersecurity workforce in responding to cyber attacks effectively while minimizing possible damage to the cyber-physical systems. Furthermore, the human factors of both attackers and defenders change when working in groups. Examples include organized cyber criminals with political and economical intentions to damage the peer competitive organizations' infrastructure. Subsequently, defenders who work together have better understanding of cyber attacks and their eco-systems and have higher chances of success to respond to cyber criminals in a united and timely manner.

The *second* major problem with the existing competition-based learning tools and educational materials is that these tools are less retrofitted with educational mindsets and objectives when the primary purpose is to develop and explore a certain set of psychological skills for trainees. It is quite common and well-established that an effective educator, prior to teaching any materials to students, should identify a set of skills that the instructor wants the students to gain once they complete the course. The development of a skill set pertaining to cognitive and behavioral aspects of students, when playing the roles of attackers and defenders, is one of the major targets of this research work.

This paper investigates the effectiveness of competition-based training on students' learning. The paper reports the satisfaction results of participants attending a two-day training workshop where students, who played the role of blue teams, compete in obtaining higher scores. The results show that the competition-based training can be effective if it is delivered structurally with respect to the teams' level of preparation as well as the contents of each training and competition sessions.

The remainder of this paper is organized as follows: Section II reviews the state-of-the-art of competition-based cybersecurity education. Section III introduces Tracer FIRE, a competition-based digital forensics tool, designed and developed by Sandia National Laboratories. Tracer FIRE was used in the workshop. The structure and design of the workshop is described in Section IV. Sections V and VI report the evaluation strategies along with the results of the workshop, respectively. Section VII concludes the paper.

II. Competition-Based Cybersecurity Education

There are a relatively good number of tools designed for training cybersecurity practices through competitions. Deterlab [1] is an open experimental environment with its primary goal to advance cybersecurity research and education. The Deter project also targets improving and redefining methods, technology and infrastructure for developing cyber defense technology [2]. As a learning facility, Deterlab enables security educators to offer their students realistic and hands-on experiences in cyber security. A key feature of Deterlab is the reusability nature of lab exercises that have been developed by the Deter project team. Deter's online education portal enables instructors to select, design, grade exercises and manage students' accounts [3].

The Global Environment for Network Innovations (GENI) project provides a collaborative virtual laboratory for networking and distributed systems research and education [4]. The tool supports scalable experimentations on shared infrastructure through virtualization or partitioning components into distinct resource sets. It also provides access to multiple and distinct test beds for experimenters [5].

The Remote Access Virtualized Environments (RAVE) project provides remotely accessible isolated lab environments, allowing cybersecurity students from a wide range of institutions to use the facility and enrich their educational hands-on experiences in defending digital assets [6]. The educational model, implemented by the RAVE project, creates shareable virtual environments built to support many institutions.

CyberCIEGE is an interactive video game, developed for information assurance awareness training [7]. The case studies embedded in CyberCIEGE are extensible through use of a scenario development language that allows instructors to create and customize their own game scenarios. Using this tool, students play the role of decision makers for some enterprises. The game includes over twenty scenarios, which give students series of choices and thus practices. Their choices potentially affect the security of enterprise assets [8]. CyberCIEGE allows players to deploy a variety of means to enforce security policies including authentications, and access controls [9].

Cyberprotect is an interactive game hosted by social networking sites with the purpose of creating awareness of information security threats and vulnerabilities. This game is designed for specific audiences, who have background knowledge in networking technology [10]. The game has a comprehensive database of questions to evaluate the player's knowledge after each level [11].

The National Center for Systems Security and Information Assurance (CSSIA) is an Advanced Technological Education program funded by the National Science Foundation. CSSIA has provided students with real-world learning experiences in network security. This has been achieved through several program's improvements including: (1) enhanced cyber security skills' events and competitions, (2) built a national infrastructure to deliver faculty workshops, (3) established mentoring programs, and (4) developed national infrastructure models for skills and learning based on the creation of scalable and affordable virtual lab environments [12, 13].

The Iowa State University Information Assurance Center, in association with Internet-Scale Event, Attack Generation Environment (ISEAGE), and Information Assurance Student Group (IASG) hosts five Collegiate Cyber Defense Competitions (CDC) every year. They also run a combination of cyber security competition and security workshops for In-formation technology professionals and university faculty, who want to learn on how to host their own CDC [14, 15].

III. TracerFire: A Competition-Based Tool

Tracer FIRE [21], Forensic Incident Response Exercises, is a digital forensic and incident response puzzle solving competition developed by Sandia and Los Alamos National Labs in 2009 to address the growing need for more highly skilled cybersecurity practitioners in the United States.

Many of the existing cybersecurity educational initiatives are centered on basic and simple concepts such as documenting compliance with policies and audits. Tracer FIRE is developed by a team of computer scientists, cognitive experts, and cybersecurity practitioners in order to *motivate students to learn the complex problem-solving skills* necessary to become a top-notch incident response analyst with the ability to recognize adversarial behavior, intervene, and mitigate malicious actors on US Government and private sector networks [21].

Students competing in Tracer FIRE are usually assisted and mentored by a team of cybersecurity experts who help and guide students in learning the various critical skills such as malware reverse engineering, forensic analysis of infected systems, network protocol analysis, and packet capture analysis. The scenarios created for Tracer FIRE are based on real life incidents provided by the Sandia's Cyber Incident Response Team. The malware artifacts are modified and actual victim names have been removed to maintain privacy but the technical details of the methods used are kept intact to help students learn through manipulation of live environments with tools used by the professional analysts.

Texas Tech University is currently collaborating with the Sandia National Laboratories to help pilot an educational

initiative to integrate competitions and games into the cybersecurity curriculum based on the Tracer FIRE model of competitions in order to engage and motivate students. As part of this initiative, Sandia is conducting a Laboratory Directed Research and Development (LDRD) funded effort to study how effective Tracer FIRE is at distinguishing the behaviors and performance of expert cybersecurity analysts versus novice cybersecurity analysts using a combination of cognitive science and neuroscience methods. This study can be helpful to researchers interested in improving the quality of education and training techniques used within game-based initiatives such as Tracer FIRE and thus build a more advanced capacity of professionals nationwide.

The US Department of Energy (DOE), the operating owner of the Sandia National Laboratories, is funding a Minority Serving Institute Partnership program to build a consortium of minority serving institutes focused on establishing a cybersecurity pipeline of students from underrepresented minorities that are educationally qualified to compete for cybersecurity research and technology jobs at the DOE National Labs and within US industry. Tracer FIRE has been selected as a prime tool to help facilitate the cybersecurity curriculum that is being developed by the educational institutes within the consortium. Texas Tech University is a partner in this effort as an evaluator to help measure the effectiveness of this educational initiative, in particular the curriculum and tools such as the use of Tracer FIRE as an approach to engage students and enhance their learning outcome.

IV. COMPETITION-BASED WORKSHOP

The project investigators with the help of the Sandia National Laboratories' research team organized a competition-based cybersecurity training workshop. In addition to utilizing the existing open source digital forensics tools, e.g., autopsy [22], the workshop organizers also offered training sessions based on the Tracer FIRE tool to let the participants experience more advanced and technical aspects of system security and in particular memory and disk forensics. Using Tracer FIRE with the requisite system hooks, we could develop instruments and collect data to better understand what students were doing during the exercises. This also allows Sandia National Laboratories, the stakeholder of the Tracer FIRE, enhance the Tracer FIRE server and game engine to closely integrate with the objectives of this effort. This study focused on investigating the effectiveness of competition-based training for the college students. The ultimate goals are (1) enhancing the competition-based training tools with educational thinking in mind, (2) identifying skills needed to become better and more effective cyber defenders, and (3) creating instructional modules to be taught prior to completion-based trainings.

A. Methods

The participants of the two-day workshop were divided into teams of 3 – 4 students, each team acting as a blue team. The participants were informed about the puzzle-solving activities and as they solved challenging problems they were given more pieces of a hidden story. Solving each challenging problem would reveal a portion of the hidden stories and each piece of puzzle was contained information and cues necessary for solving the next challenging problems.

For solving challenging questions, the participants needed to utilize some other open source digital forensics tools such as autopsy [22], and an open source PDF analyzer. Performance comparisons occurred at the level of the teams. Teams received scores for solving each challenging problem. The team that solved the most challenging questions received higher scores and secured the win.

B. Subjects Recruitment

Subjects were recruited from undergraduate and graduate students at Texas Tech University. The requirements for participation included: i) had a GPA of at least 2.75, ii) had taken courses such as: Operating Systems, Computer Architecture, Computer Network, and Programming Languages, iii) had an interest in cyber security, and iv) had experience with team-based activities. Participants were asked to complete a consent form to ensure they understood the purpose of the study and the workshop.

C. Procedure

Subjects were asked to complete a demographic questionnaire that asked the participant about their age, gender, educational background, years of experience with computers and years of experience with cyber security. Participants were also requested to complete a questionnaire assessing computer and security background knowledge. This information was intended to inform team selection. The objective was to have balanced teams with respect to the knowledge and experience of team members. Given that all of the participants were students who already had good experience with computer science and security, we decided to form the teams randomly.

The students participating in the two-day workshop were divided into groups acting as blue teams detecting cyber threats and utilizing defending strategies to protect their cyber systems.

D. Other Open Source Digital Forencis Tools Used

As indicated earlier, to solve the challenges participants needed to have cyber security knowledge and were allowed to use some available disk and memory digital forensics tools. Therefore, participants were exposed to existing open source tools such as i) Hex Editor; to edit and read files in hexadecimal format, ii) Autopsy; to perform disk analysis on disk image files, and iii) PDF scanner; to scan PDF files for potential malware and embedded Java scripts.

E. Tracer FIRE Exercises

Tracer FIRE is an assessment tool with various exercises that serve as testing sessions to measure the effectiveness of teaching methodologies. In a typical case, participants should be divided into teams, each receiving different forms of training. For instance, using Tracer FIRE it is feasible to test whether teaching based on learning through tools is superior to lecture-based training and vice versa.

We did not set out to examine which mode of instruction was effective. Rather, the objective of this project was to assess the effectiveness of competition-based training in general on students' learning. To this end, the formed teams received similar training and formal lecturing accompanied by similar hands-on experiences.

Each team was asked to solve multiple disk and memory forensics challenges to receive points. The challenges were built around a series of multi-stage attacks to the same network infrastructure.

At the beginning of the exercise, the participants were told that there were elements of a story embedded within the upcoming series of challenges. Solving each challenge offered a clue for revealing some parts of the embedded story and in helping solve the subsequent challenge. Upon solving challenges, teams were able to reveal the hidden story and puzzle scenario that could assist in resolving the upcoming challenges [20].

V. Evaluation of The Workshop

An evaluation of the cyber security workshop was conducted using a repeated measure ANOVA with five dependent variables: (i) *cyber security knowledge*, (ii) *team-based skills knowledge*, (iii) *confidence in cyber security skills*, (iv) *confidence in team-based skills*, and (v) *workshop satisfaction*. Eighteen participants participated in the workshop on the first day and seventeen participated on both days.

How knowledgeable are you in each of the following areas?	Not at all		Somewhat knowledgeable			Very knowledge-able
1. forensic analysis of infected systems	1	2	3	4	5	6
2. tactical strategies for cyber security risk detection	1	2	3	4	5	6
3. incident response analysis	1	2	3	4	5	6
4. packet capture analysis	1	2	3	4	5	6
5. malware reverse engineering	1	2	3	4	5	6
6. situational awareness of cyber attacks	1	2	3	4	5	6
7. rapid response cyber forensics	1	2	3	4	5	6
8. analysis of exploits	1	2	3	4	5	6
9. memory forensics	1	2	3	4	5	6
10. host artifacts of an attack	1	2	3	4	5	6
11. team-based collaboration and communication (not technical content rather a social skill)	1	2	3	4	5	6
12. team-based competition (not technical content, rather a social skill	1	2	3	4	5	6

Figure 1. Cyber security survey knowledge items.

How confident to you feel about being able to do each of the following tasks?	Not at all		Somewhat confident			Extremely confident
1. analyze infected systems	1	2	3	4	5	6
2. identify cyber security risk	1	2	3	4	5	6
3. mitigate cyber attacks	1	2	3	4	5	6
4. conduct packet capture analysis	1	2	3	4	5	6
5. reverse engineer malware	1	2	3	4	5	6
6. develop tactical plans to identify cyber security infrastructure risk	1	2	3	4	5	6
7. use data analyze threats and make predictions	1	2	3	4	5	6
8. conduct analysis of exploits	1	2	3	4	5	6
9. communicate effectively in collaborative activities	1	2	3	4	5	6
10. participate meaningfully in team competitions	1	2	3	4	5	6

Figure 2. Cyber security survey confidence items.

How satisfied are you with each of the workshop's presentations?	Not at all		Somewhat satisfied			Extremely satisfied
1. Rapid Response Cyber Forensics and Analysis of Exploits	1	2	3	4	5	6
2. Tracer FIRE, Part I	1	2	3	4	5	6
3. Tracer FIRE, Part II	1	2	3	4	5	6
4. Memory Forensics and Host Artifacts of An Attack	1	2	3	4	5	6
5. Tracer FIRE, Part III	1	2	3	4	5	6
6. Team Final Briefings	1	2	3	4	5	6

Figure 3. Cyber security workshop satisfaction items.

Analyses were conducted on the reports of the seventeen participants for which there was complete survey data.

A. Participants' Background

The majority of the participants were male (13 of 18) and Texas Tech University students (10 undergraduate, 6 graduate). Two participants were students at a neighboring private university. The ethnic background of the participants was as follows: 7 white, 6 Asian, 3 Hispanic, 1 African-American and 1 female participant declined to identify her ethnicity. The great majority of participants (15 of 18) identified Computer Science as their major; two were studying Information Systems and Technology; one was studying Software Engineering.

B. Participant Survey

Participants were asked to complete a short survey to report their perceptions of knowledge and confidence related to cyber security targeted by the Cyber Security Workshop. Participants were also asked to report their overall satisfaction of the workshop. Participants reported knowledge and confidence perceptions on six-point Likert scales at three separate time points during the two-day workshop: (a) Time 1 prior to the start of the workshop, (b) Time 2 at the conclusion (i.e., the closing session) of the first day of the workshop, (c) Time 3 at the conclusion (i.e., the closing session of the workshop) of the second day of the workshop. Participants reported their overall workshop satisfaction at the end of first (Time 1) and second (Time 2) days of the workshop.

- The cyber security knowledge variable was calculated by averaging the first 10 items of the Cyber Security Workshop Survey (see Figure 1), which reflected the intended content of the workshop:
- The team-based knowledge items were calculated by averaging responses to items 11 - 12 presented in Figure 1;
- Confidence in cyber security knowledge and team-based skills variables were calculated by averaging responses to the first eight items presented in Figure 2;
- Team-based skill confidence was calculated by averaging responses to items nine and ten as presented in Figure 2;
- Finally, the Time 1 workshop satisfaction variable was based on the average of the first 2 items of Figure 3 and the Time 2 variable was based on the average of all the items presented in Figure 3.

C. Open Ended and Interview Questions

To supplement participant reactions to the workshop at the conclusion of the second day of the workshop, participants were also asked to identify:

(1) The most important concept/idea or skill related to cyber security;
(2) Evidence in support of the concept identified as the most important; and
(3) Other valuable concepts and skills needed for maximizing cyber security.

In addition, a small sample (6; 3 male, and 3 female) of participants was asked to participate in a brief structured interview. These participants were asked to expand on their impressions of the workshop, what they found most and least helpful, what could be added, how the game challenges helped them gain skills and how they would use what they learned.

VI. Results

This section reports the results of the analysis along with the outcome of the interview questions and survey.

A. Survey Responses

As presented in Table 1, participants reported low levels of cyber security knowledge and confidence prior to the workshop participation (Time 1). The average mean for cyber knowledge and confidence was 1.84 and 2.37, respectively, indicating a very low level of knowledge and confidence at Time 1. Team-based skill knowledge and confidence was slightly higher with a mean of 3.71 for both of these variables at Time 1.

These average means were increased at the end of the first day of the workshop (Time 2). The cyber security knowledge and confidence at the end of the first day of the workshop were 2.82 and 2.99, respectively. The data show 53% and 26% increases in cyber security knowledge and confidence, respectively, at the end of first day of the workshop.

At Time 3, participants reported significantly higher levels of cyber knowledge, team-based knowledge, and cyber skill confidence than Time 1. The cyber security knowledge and confidence level were increased to 3.56 and 3.57, respectively. The effect size (η^2) indicates that magnitude of effect was moderate (.54) which is significant given the small sample size. More precisely, the cyber security knowledge had an increase of 93% and 26% compared to Time 1 and Time 2, respectively. Similarly, the confidence levels showed 50% and 19% increases compared to Time 1 and Time 2, respectively. This suggests that despite the short workshop length, overall, the participants left the experience believing they gained some knowledge and skills in implementing cyber security analyses in team situations.

However, differences between levels of team-based skills confidence were not significantly different for any of the paired comparisons tested (Time 1 and Time 2, Time 2 and Time 3, and Time 1 and Time 3), (i.e., p-value=0.140). This could be attributable to the duration of the workshop, as more team-based activities may be necessary to increase confidence in this area particularly since they came to the workshop with higher self-reports of team-based skills than other areas,

It is also important to note that the overall means at Time 3 were still not high, as means in the 3 and 4 range indicated "*somewhat knowledgeable*" and "*somewhat confident*." This is likely due to the low levels of initial knowledge reported. It would *require more than two days* to acquire the knowledge and skills necessary to perceive oneself as a master of cyber security.

B. Open Ended and Interview Responses

Of the 16 participants who responded to the open-ended items, 11 (69%) indicated that "*analysis*" was the most important idea they took away from the workshop. This was the response with the highest frequency. An example of this response is as follows "*understanding how to approach the problem*," and "*…analyzing files to discover malicious code*."

The response with the second highest frequency was the "*importance of use of appropriate tools*" to be able to conduct such an analysis, followed by understanding the mindset of the hacker as in "*thinking like an adversary*," and "*learn the relevant thought process*."

In response to evidence in support of the central idea, the most frequent response type (7 of 16 or 44%) was directed at the process for monitoring potential threats as in the following response "*Hard drive can be analyzed to determine how malware works…. and analyzed to provide evidence of criminal activity*." Only two responses revealed a principled understanding of cyber security that went beyond a list of processes featured by the workshop. An example of principled understanding is represented in the following response:

"*Most security vulnerability is a result of network traffic. If there was a tool to monitor that in real time, I think it would mitigate malicious activity*."

Table 1. The satisfaction results of the training workshop. * Mauchly's test of sphericity was significant. Therefore, Greenhouse-Geisser adjustment was used to determine significant levels.

Variable	Time 1 M	Time 1 SD	Time 2 M	Time 2 SD	Time 3 M	Time 3 SD	F-Test	*p*	η^2	Bonferroni
Knowledge Self-Reports										
Cyber Skill Knowledge	**1.84**	**.94**	**2.82**	**1.03**	**3.56**	**1.31**	**18.42* (1.25, 20.06)**	**.000**	**.535**	**T1<T2, T2<T3, T1<T3**
Team Skills Knowledge	**3.71**	**1.49**	**4.18**	**1.24**	**4.88**	**.84**	**5.39 (2, 32)**	**.010**	**.252**	**T2<T3** **T1<T3**
Confidence Self-Reports										
Cyber Skill Confidence	**2.37**	**1.10**	**2.99**	**1.21**	**3.57**	**1.37**	**6.06* (1.25, 19.94)**	**.018**	**.275**	**T1<T3**
Team Skills Confidence	**3.71**	**1.55**	**4.06**	**1.36**	**4.56**	**1.18**	**2.24* (1.40, 22.39)**	**.140**	**.123**	**N/A**
Workshop Satisfaction										
Satisfaction	**3.74**	**.94**	**4.35**	**1.16**	**N/A**		**10.84* (1, 17)**	**.004**	**.39**	**N/A**

C. Workshop Satisfaction

Finally, although the satisfaction means increased from Time 1 to Time 2, participants expressed less than enthusiastic satisfaction of the delivery of the workshop. A mean of 4.35 represents being "*somewhat satisfied*." Four of the six participants who were interviewed indicated the need to have more detailed instructions and parameters for workshop activities, especially the game challenge situations. Three participants expressed some frustration with the organization of the workshop. However, all of those interviewed expressed *the utility of the game scenario in helping them appreciate the mindset of potential threats*. They cited the teamwork opportunities as a key to gaining skills in monitoring cyber threats. Further, *all six interviewees also indicated they would be able to use what was learned in applied situations*.

D. Lessons Learned

As the evaluation and results of the training workshop indicate the competition-based training, using an assessment tool such as TracerFIRE, can be an effective educational tool if employed and implemented properly. The results showed that:

- The participants liked the competition-based learning incorporated into the workshop. The competition atmosphere stimulated their motivations to solve more challenges and thus stand in better rankings.
- The team-based activities were well received by the participants. As per the results of interviews and open-ended questions, it was observed that team-based activities highlighted the importance of communication skills in solving a common challenging problem shared by teammates.
- The participants reported that they actually learned more materials through completion-based training and using the assessment tools. More importantly, it was observed that the participants learned from their teammates while working on a common challenging problem.
- The participants showed their interest in the topic, i.e., digital forensics, and indicated that taking such a course would be very a valuable and informative course for

students. It may suggest the importance of memory and disk forensics on cyber security research and practices and in particular to malware detections.

On the other hand, there were some other concerns regarding the structure, organization, and delivery methods of the workshop:

- It was noticed that the participants needed more formal lecturing prior to being exposed to the challenging questions. The reason might be the due in part to lack of sufficient background knowledge in the underlying topic, i.e., digital forensics.
- There were some concerns regarding the timing and length of the competition sessions. Each competition-based session was around 3 to 4 hours long. It was noticeable that the participants needed some breaks during these long sessions. Dividing the competition sessions into smaller chunks would enhance the productivity and preserve excitement of participants.

The valuable take-away lessons from the workshop could be as follows:

- Develop clear and well-designed competition-based sessions. Knowing the agenda and objective of each session would help in increasing the focus of the participants and the expectations.
- Develop related instructional modules and deliver formal lectures along with hands-on experiences prior to each competition-based session.
- Provide a test environment (e.g., a virtual machine) where related software digital forensics tools would be exercised before the competition.
- Shorten the competition-based sessions. Longer competition sessions may deteriorate the effectiveness of the training.
- Each session must have a clear structure and incorporate i) formal lecturing, ii) hands-on experiences, and finally iii) competition-based activities.

VII. Conclusion and Future Activities

Taken together, the survey and interview data suggests that content of the workshop was viewed as valuable to participants, and therefore future efforts should maintain these areas of cyber security as targets. However, the delivery may need some additional structural adjustments to increase participants overall satisfaction and confidence in applying the processes presented. The most evident implication is the need to expand the duration length so that participants coming with minimal to no prior experience or knowledge in this field have sufficient time to process the information. The workshop would also help participants achieve workshop goals if clear goals and objectives were identified and communicated to participants. Once these are identified, workshop activities should be appropriately paced and sequenced so that all participants leave the experience with increased knowledge, confidence and skills. For each workshop component, clearer instructions and parameters would help participants come away from the experience with these perceptions.

Acknowledgment

This work is supported by the National Science Foundation under award number DGE-1516636. The authors would like to thank the Sandia National Laboratories for offering the professional workshop. Thanks to Dr. Fethi Inan for the discussions about the workshop.

References

[1] B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hilber, C. Barb, and A. Joglekar, "An integrated experimental enviornment for distributed systems and networks," ACM SIGOPS Operating Systems Review, 36.SI:255-270, 2002.

[2] J. Mirkovic and T. Benzel,"Teaching cybersecurity with Deterlab," IEEE Security & Privacy, 10.1:73-76, 2012.

[3] J. Mirkovic, T.V. Benzel, T. Faber, R. Braden, J.T. Wroclawski, and S. Schwab, "The Deter project: Advancing the science of cybersecurity experimentation and test," In Proceedings of the IEEE HST'10 Conference, Waltham, MA, November 2010.

[4] Geni exploring networks on the future. GENI, Feb 2014.

[5] L. Peterson, S. Shenker, and J. Turner, "Overcoming the Internet impasse through virtualization," Computer, 2005.

[6] J. Quan, N. Kara, and B. Hay, A mutualiztic security service model: Supporting large-scale virtualized enviornment," IT Professional, 13(3): 18-23, 2011.

[7] J. Jones, Y. Xiaohong, E. Carr, and Y. Huiming, "A comparative study of cyberceige game and department of defense information assurance video," In Proceedings of IEEE SoutheastCon, 2010.

[8] M. Thompson, and I. Cynthia, "Active learning with cyberseige video game," In Proceedings of the 4th Conference on Cyber Security Experimentation and Test. USENIX Association, 2011.

[9] C.E. Irvine, and T. Michael, "Teaching objectives of a simulation game for computer security," Technical Report, Naval Postgraduate School, Monterey CA, 2003.

[10] W. Labuschange, N. Veerasamy, I. Burke, and M. Eloff, "Design of Cyber security awareness game utilizing a social media framework," In Information Security South Africa (ISSA), 2011.

[11] CyberProtest, Web. Feb. 2014.

[12] CSSIA NSF ATE Center, Feb. 2014.

[13] P. Hills, "CSSIA in training faculty online in cyber security curriculum, Feb. 2014. http://www.prweb.com/releases/facultydevelopment/CSSIA/prweb11350342.htm

[14] Cyber Defense Competition Workshop, Feb. 2014.

[15] ISU Inf As Student Group, National Cyber Defense Competition, 2014.

[16] B. Anderson, A. Carajal, J. Jarocki, J.T. McClain, K. Nauer, T. Reed, S.Stevens-Adams, and C. Forsythe, "Enhanced training for cyber situational awareness in red versus blue team exercieses," Technical Report, Sandia National Laboratories, 2012.

[17] T. Reed, K. Nauer, and A. Silva, "Instrumenting competition-based exercieses to evaluate cyber defender situation awareness," Technical Report, Sandia National Laboratories, 2013.

[18] T. Reed, K. Nauer, and A. Silva, "Cognitive and human performance research applied towards cyber security training and education," Technical Report, Sandia National Laboratories, 2013.

[19] A. Gonzalez-Prendes, and S. M. Resko, "Trauma: Contemporary Directios in Theory, Practice, and Research – Chapter 2: Cognitive Behavioral Theory," Sage Publications, May 2012.

[20] A. Carbajal, S. Stevens-Adams, A. Silva, K. Nauer, B. Anderson, C. Forsythe, "Enhanced Training for Cyber Situational Awareness in Red versus Blue Team Exercises," Technical Report, Sandia National Laboratories, SAN 2012-8812 P, September 2012.

[21] http://csr.lanl.gov/cyberfire/

[22] Autopsy: An Open Source Digital Forensics Tool; http://www.autopsy.com/