Novice Cybersecurity Students Encounter TracerFIRE: An Experience Report

Nolan E. Frost
nef4601@uncw.edu
Computer Science

Geoff Stoker
stokerg@uncw.edu
Information Systems

University of North Carolina Wilmington
Wilmington, NC 28403

Abstract

Integrating hands-on learning into a competitive cybersecurity exercise is known to be a popular and potentially powerful way to motivate experiential learning in computer and network security (Childers, et al., 2010; Fanelli & O'Connor, 2010; Vigna, et al., 2014; Siami Namin, et al., 2016). In addition to having taken relevant computer science (CS) and/or information technology (IT) classes, competitive cybersecurity exercise participants typically conduct specific preparation activities based on known technical expectations of the exercise. It is also common, in team events, for some portion of the team to have prior experience navigating the rigors of the event. Over the weekend of February 22-23, 2020, eight students from the University of North Carolina Wilmington (UNCW), with no prior competitive cybersecurity event experience and little preparation attended their first-ever cybersecurity competition – Tracer FIRE 9. In this paper, we describe that experience and relate how experiential learning made it valuable even for a group with very little previous exposure to cybersecurity-specific education.

Keywords: Cybersecurity, Competition, Tracer FIRE, Experiential Learning

1. INTRODUCTION

The University of North Carolina Wilmington (UNCW) has maintained an active cyber defense club (CDC) since academic year 2011-2012. Over the years, the CDC has variously met once a week or once every two weeks during the fall and spring academic semesters to discuss cybersecurity topics, share presentations on tools, hear from guest speakers, and prepare for upcoming cyber defense competitions. With a current undergraduate population of ~14,000, yearly membership has ranged as high as about 40 and regular club meetings often draw somewhere between 15 and 20, though some events have many more attendees and some meetings have far less.

Though the CDC has sent teams to compete in several different competitions in recent years like the Department of Energy's (DOE) CyberForce, Palmetto Cyber Defense Competition (PCDC), and Wicked6 Cyber Games, the primary competition focus since club inception has been the Southeast Collegiate Cyber Defense Competition (SECCDC). The SECCDC is a two-step gateway for one team from the southeast region to make it to the National CCDC ("SECCDC," n.d.). First, there is a virtual preliminary qualifier that schools participate in from their home campus in February. This year, 2020, there were 34 teams that competed. Second step is a (typically) on-site competition for eight teams in Atlanta at Kennesaw State University in early April. UNCW's

CDC has participated in every virtual qualifier held each spring semester from 2012 to 2020 and made it to the on-site regional competition 7 times. So, the SECCDC is uppermost in CDC members' minds with the most experienced and senior members traditionally the ones who prepare for and attend the competition.

This year, we received an invitation to the Tracer Forensic Incident Response Exercise (FIRE) 9 event at North Carolina Agricultural and Technical State University (NC A&T) on February 22nd and 23rd, 2020 which was the same weekend as the SECCDC virtual qualifier. The timing conflict and prioritization of the SECCDC effort by the most experienced CDC members meant that attending both would necessitate sending a team to Tracer FIRE where no member had any previous cybersecurity competition experience. As well, many of the members attending were new to the club with a semester or less of meeting attendance. Additionally, with no CDC member having had prior Tracer FIRE experience and surprisingly little information readily available on the web about what to expect or how to prepare, the team was unclear about how best to get ready for the event.

The purpose of this paper is three-fold. First, we wish to provide an update to the Tracer FIRE participant experiences that can be readily found online in the hopes that it will benefit future attendees. Second, we will provide a first-hand experience report that first-time attendees should find particularly useful and demystifying. Third, in the spirit of other's efforts (Rege, 2015), we will provide a light introduction to the concept of experiential learning and offer a brief reflection of our Tracer FIRE experience though that lens.

In section 2 of this paper, we report on Tracer FIRE 9 (TF9). Section 3 briefly describes experiential learning and discusses its relationship to our TF9 experience. Section 4 presents a reflection and some recommendations, while section 5 concludes.

2. TRACER FIRE

Brief Background

Originally created for the DOE in 2009 ("Security-savvy," 2010), Tracer FIRE was developed by Sandia and Los Alamos National Laboratories to train the critical skills needed by DOE cybersecurity incident responders and analysts (Treece, 2020). In more recent years, Sandia National Laboratories (SNL) has assumed responsibility for the program and primarily uses it to conduct educational outreach to students interested in cybersecurity.

Tracer FIRE 9 Overview

Tracer FIRE 9 was a two-day event that focused on both training and competition aspects of digital forensics and incident response. The event was orchestrated and administered by cybersecurity professionals from SNL who constructed the competition challenges from the ground up. SNL described it as a forensic incident response exercise offered in a hands-on training format that is live, immersive, and interactive (*Tracer FIRE*, 2020). The training focused on developing incident response skills using four main software applications: Ghidra, Security Onion, Autopsy, and Volatility.

The TF9 exercise simulates a live incident response experience that is broken down into three levels:

1. perception – an incident responder detects something has happened.
2. comprehension – incident responders look into what actually happened and determine the nature of the adversary and the type of attack.
3. prediction – analysts determine what the adversary was targeting and attempt to predict whether the victim will be targeted again or not.

Tracer FIRE was advertised as an event where students would investigate advanced persistent threat (APT) style adversaries throughout the simulation by focusing on the questions:

- Who is an adversary?
- How did they get in?
- What did they want, and did they succeed?
- How do we prevent recurring incidents?

Our TF9 Experience

As mentioned earlier, with the conflict between the SECCDC virtual qualifier and TF9, volunteers for TF9 attendance were sought and two teams of four created from among the inexperienced members of our CDC.

Relevant demographic information for the eight members breaks out as follows:

- All undergraduates
- 2 females; 6 males
- 1 Hispanic; 1 black/African American; 6 white/Caucasian
- 3 IT majors; 5 CS majors

Both teams met once, about a week before the event, for about two hours to try and gather information on the structure of the event or what

technical knowledge might be especially beneficial to know for the competition and any hints on how to prepare. Eight people's web search efforts turned up surprisingly little specific information about Tracer FIRE useful to first-time attendees. While we found several academic papers exploring various concepts researched during Tracer FIRE execution (Anderson, et al., 2012; Carbajal, et al., 2012; Reed, et al., 2013; Stevens-Adams, et al., 2013; Abbott, et al., 2015; Perry, et al., 2017), we found little about the actual exercise itself. The most we were able to find out was that we would be learning about and using the tools Ghidra and Security Onion. Only one student had previously heard of Ghidra and while most had at least heard of Security Onion, few had any experience using the application suite and none had any meaningful experience.

Once both teams arrived at NC A&T for the first day of the event, we were briefed on what would be happening each day. There were 27 student attendees in total, hailing from 6 different North Carolina institutions: NC A&T, Elon University, East Carolina University (ECU), University of North Carolina Greensboro (UNCG), High Point University (HPU), and UNCW. The first thing that the event administrators from SNL did that seemed to surprise everyone in attendance was to randomly split us up into new teams with no regard for the teams with which we had registered. All attendees were split into six teams total, so two teams had two UNCW team members and the other four teams had one UNCW member each. Some teams had 4 members, and some had 5 since there were 27 students in total.

The explanation of our TF9 experience that follows is specifically written to provide information useful to those looking to demystify the structure and scaffolding of Tracer FIRE events without revealing details of the actual TF9 scenario and associated challenges. We hope that this balance will be both enlightening and non-spoiling (i.e. no "spoiler alert" warning required).

Day 1

The first day followed the schedule in Table 1. For the first half of day one, we were given a quick crash course on the idea of incident response, as well as how to use email, Ghidra, Security Onion, and Autopsy in an incident response capacity.

As far as Simple Mail Transfer Protocol (SMTP) and email extraction goes, we learned what information is included in email headers, how to sort network traffic in another tool like Security Onion or Wireshark to filter out email (SMTP) traffic, and how to use emails and the times at which they are sent to identify linked packets and other network traffic involved in an incident. We did not learn skills for any new software in conjunction with the email lesson, but the information we covered about email was essential for the competition because of the amount of information lucrative to the competition that had to be found through email files.

Saturday, February 22, 2020	
0830-0900	Introduction
0900-0930	Cybersecurity and Incident Response
0930-0945	Setup and Configuration
0945-1045	Introduction to Ghidra
1045-1100	Break
1100-1115	SMTP and Mail Extraction
1115-1145	Introduction to Security Onion
1145-1300	Lunch Provided
1300-1330	Disk Forensics with Autopsy
1330-1345	TF9 Story Overview and Setup
1345-1700	TF9 Exercise

Table 1 – TF9 Day 1 Schedule

The first software application covered in the training was Ghidra. It is an open source software reverse engineering tool developed by the National Security Agency's (NSA) Research Directorate which released the binaries to the public in March 2019 at RSA Conference and then released the source code in April. It is also known as a decompiler because its main function is to decompile executable programs and convert them to source code for analysis. It is used by many cybersecurity professionals to analyze malicious code and malware, and can be used to identify potential vulnerabilities in a network or system. We used Ghidra later in the competition to analyze an electronic product's firmware in order to determine the acceptable ranges for the product's diagnostic values.

Following Ghidra, we were taught the basics of SecurityOnion. SecurityOnion is described on its website as a:

> free and open source Linux distribution for threat hunting, enterprise security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Zeek (formerly known as

ISSN: 2473-4901
v6 n5337

Bro), Wazuh, Squil, Squert, CyberChef, NetworkMiner, and many other security tools (SecurityOnion).

During the event we only scratched the surface of what you can do with all of the tools included in the SecurityOnion application suite and focused most of our time on the Elasticsearch, Logstash, Kibana (ELK) stack and Squert. Elasticsearch is a search and analytics engine that works well with complex search features and requirements. Kibana is a data visualization dashboard for Elasticsearch and Logstash is used to process and transform data before storing and logging it. Squert is used to query and view event data and is often used to analyze packet capture (pcap) data. These tools were used during the competition to analyze network traffic and event data, as well as data from various types of logs and files that were compatible with the tools within SecurityOnion.

The final application that was covered in the day one training is Autopsy. It is an open source digital forensics platform used to investigate what happened on a computer. It "analyzes major file systems by hashing all files, unpacking standard archives, extracting any exchangeable image file format (EXIF) values, and putting keywords in an index" (Autopsy). Users can then search the data for recent activity or with other search criteria, and generate reports summarizing the data. During the competition, we used Autopsy to inspect the hard drives and desktop volumes of various characters' computers in order to find information related to the incidents being investigated.

Training for the information covered above ran from 0830 to 1330 (1:30pm). The remainder of the first day was spent on the competition. For the competition, everyone connected their personal laptops to an external server via ethernet and used the same virtual machine on which all of the required software had been pre-installed. All teams were briefed together on the competition format, which included a series of challenges wrapped within a complementary fictional business storyline that included cybersecurity events. The challenges were made available to all teams at the same time.

There were five separate challenge tracks, each consisting of numerous individual challenges or mini "capture the flags" (CTF) where you had to identify a specific piece of information and enter it in order to unlock the next challenge. The challenges for each track had to be done in order within the track. Each track of challenges represented a different incident, and you would have to complete the entire track in order to uncover all of the information and get a full picture of what happened with the incident.
Points for each challenge were awarded based on how many of the other teams completed that specific challenge. If your team was the only team that solved the challenge, then your team would be awarded 100 points. For every other team that came along and solved the challenge, the points that you were awarded decreased. There were also optional hints that would reduce the amount of points potentially awarded for that specific challenge if your team used them.

The event administrators displayed a leaderboard showing each team's score for the entire time that we were working on the first day. The event administrators also walked around and were available to answer questions if you were really stuck or needed clarification. The strategy that most teams decided to follow was to assign a specific person to each track of challenges with teams of only four people usually either assigning their most knowledgeable person to work on two tracks or having everyone rotate to work on the remaining track when they got stuck on their own track or when they were further ahead than their teammates. At the end of the first day, the administrators locked the challenges so that no one could see the questions and potentially work ahead.

Day 2
The second day followed the schedule in Table 2.

Sunday, February 23, 2020	
0830-0900	Memory Forensics with
0900-0930	Advanced Security Onion
0930-1130	TF9 Exercise
1130-1300	Lunch Provided
1300-1600	TF9 Exercise
1600-1615	Debrief Preparations
1615-1700	Debriefs (~5 min each)
1700-1710	Debrief Point Deliberation
1710	Closing

Table 2 – TF9 Day 2 Schedule

On day two, there was only one hour reserved for training. During that hour we covered the basics of Volatility and some advanced SecurityOnion material. Volatility is an open source software tool that is used to analyze random access memory (RAM) and memory dumps (raw dumps, crash

dumps, VMware dumps). It was covered on day two because only challenges later in the challenge tracks required the use of Volatility in order to find the necessary information. One of the tracks required Volatility to be used with a crash memory dump when a device unexpectedly stopped operating.

We were then given from 0930 to 1600 (4:00pm) on day two to continue working on the competition challenges. Around lunch time we were informed that every team had to prepare and give a presentation formatted like an incident response report to executives in the companies whose incidents we were analyzing. We were told that the presentations would contribute to our overall competition scores.

The point of the competitions was to make the teams piece together the information discovered from the individual challenges in each challenge track to see the incidents from a broader perspective and gain an in-depth understanding of what actions led to each incident. Teams presented in a separate room from the competition room to a panel comprised of the event administrators and any faculty that travelled with the students. The number of points awarded from the presentation varied depending on the quality of the presentation and the score awarded, but ranged from ~5% to ~25% of most teams point totals prior to the presentation points being factored in. The final thirty minutes of day two was spent calculating the teams' total scores, announcing the final standings, and presenting the winners with their certificates, while also answering participants' questions about the exercise challenges, taking pictures, and networking.

3. EXPERIENTIAL LEARNING

Overview

In this section, we will briefly describe the background and key elements of experiential learning and relate it to our experience with TF9.

Dr. David Kolb drew on the foundational work of such well-known scholars as Carl Jung and John Dewey in developing his experiential learning theory (ELT) (Kolb & Kolb, 2013). ELT is a dynamic view of learning based on the experiential learning cycle (ELC) in Figure 1. Kolb defines learning as "the process whereby knowledge is created through the transformation of experience" (Kolb, 1984, p. 38). ELT places the learner's experience at the center of the learning process where "the center of learning is experience – your own subjective experience" (Hay Group Global, 2012).

Given the looping nature of the ELC, it can be entered at any stage; however, it might be easiest to think about starting with someone having a concrete experience (CE). This CE allows for reflective observation (RO) – what worked, what did not work, etc. These observations and reflections on them are assimilated via abstract conceptualization (AC). This often results in new ideas or the modification of old ideas. Active Experimentation (AE) then follows with the new conceptualizations being tested out. A short-hand way of thinking of the loop is: experiencing (CE), reflecting (RO), thinking (AC), acting (AE).

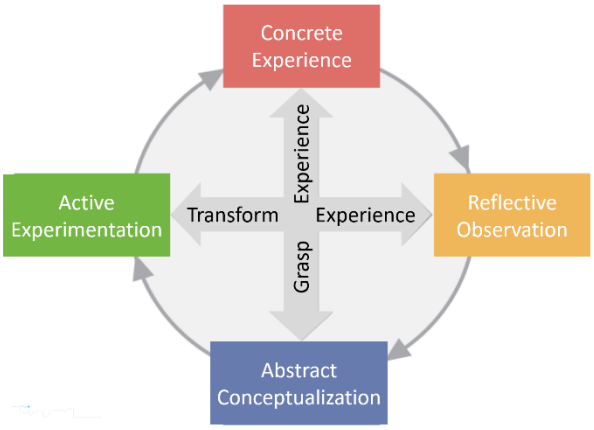

Figure 1. The Experiential Learning Cycle (Kolb & Kolb, 2013, p. 8)

While some explanatory examples we have seen of the ELC emphasize careful reflection in such a manner that it seems to imply a deliberate, non-trivial time spent apart from acting, different activities will cause a much quicker loop through the four stages – for example, someone learning a new music piece on the piano. Our experience at Tracer FIRE resembled this latter experience involving rapid loops or spirals through the ELC.

Experiential Learning Through TF9

Key to how ELT and our participation in the Tracer FIRE 9 event relate is captured beautifully in a quote from Dr. Kolb from a short YouTube video that we watched:

> As a learner, it's my experience that guides how I learn and says when I have learned something. The exciting thing about this idea is that when your experience is the center of the learning process, you are in control of it. And you are able then to take initiative and create

> the kinds of experiences that you want and that lead to learning for you (Hay Group Global, 2012).

Each of the eight UNCW participants took part in the same cybersecurity competition, but given the myriad of tasks/challenges and the random organization of all participants into teams, had tremendous freedom to self-direct their efforts, so unsurprisingly, each participant engaged with different parts of the exercise at different depths.

Below, we provide three example narratives from student attendees (not the authors) that reflect the power of Tracer FIRE in the context of ELT illustrated by individuals taking initiative for their own learning.

Kibana Commando
Kibana is a great tool for searching, viewing, and visualizing indexed data. You can create bar charts, pie charts, histograms, etc. and then analyze the underlying data visually. One of the IT majors who attended TF9 became truly enamored with Kibana. Having never seen it before, this teammate quickly acquired the rudimentary skills needed to get value from the tool and then kept pushing deeper. Anytime someone on their team wondered how to do something related to Kibana, they would dive in and figure it out. By the end of the exercise, this person was hopping around showing teammates (and occasionally folks from other teams) different tips/tricks they had learned.

Gripped by Ghidra
Ghidra is a cool tool and "gripped" definitely reflects the level of interest and attitude that one of our CS majors took towards the NSA's software tool. This teammate was the one who had heard of it prior to us conducting a search for information about Tracer FIRE the week before the event. This pre-event interest carried into TF9 and intensified once the required tasks were revealed. Such was the level of interest and confidence in their newly acquired Ghidra skills, that on the drive back to campus, this club member was already making plans to conduct a future demo and class for the CDC.

Chief Collaborator
Unlike the first two narrative examples, which centered on the strong attraction of a single technology, our third example highlights the teammate who it might be fair to say, preferred the view of the forest to the view of any particular tree. This person felt like they struggled a bit working alone on individual challenges, but as the event wore on, found that they were good at listening to other teammates talk through challenges and that the collaboration – bouncing ideas off each other – was exciting and led to challenges being solved. Often the insights still came from the person who was originally working on the challenge but talking through ideas out loud led that person to the key unlock required to solve the challenge.

Despite being cybersecurity neophytes, all eight UNCW participants had an extremely meaningful learning experience at TF9. Each came away with tangible cybersecurity skills and knowledge – primarily because Dr. Kolb's statement above was correct – with experience at the center of the learning process, we were able to take initiative and put ourselves into experiences that led to individual learning. We did not all walk away from TF9 with the same levels of knowledge about Ghidra or Kibana or Autopsy as you might expect at the end of a more traditional learning event (class, seminar, brief, etc.). But we all did leave with notably higher levels of knowledge in the subjects and aspects of the event that appealed to each of us and sparked our individual interest.

We also all left the event excited about our cybersecurity learning and full of energy and intrigue after working with cybersecurity tools hands-on for two full workdays. After reflection and discussion, our team members attributed our high levels of excitement towards the subject matter not only to the experiential learning, but also the gamification of the competition. Having accumulated point totals and a live leaderboard further incentivized all participants to progress through the challenge tracks. It provided immediate satisfaction upon challenge completion and when we could see the point total go up and/or see team rankings switch because of it.

4. REFLECTION AND RECOMMENDATIONS

All eight UNCW participants of TF9 agree that it was a worthwhile experience, that lacking greater cybersecurity skills and knowledge beforehand was not a disadvantage for learning while at the event, and that they would gladly go again if offered the opportunity. After reflection, we feel we can offer the following recommendations.

Go to Tracer FIRE
There was concern on the part of brand-new CDC members to signing up to attend a cybersecurity competition with the intimidating name of Tracer FIRE. Feelings of imposter syndrome among technology majors are common and can

discourage students from seeking out experiences that require the application of technological concepts that they have learned in school. These feelings and concerns are understandable, but do not let them stop you! Tracer FIRE is specifically designed to be a training event as well as a competition. You will be fine regardless of your current level of experience.

Think About the Presentation

Being able to assemble the different bits of information discovered during the forensic investigation portion of Tracer FIRE into a coherent incident response message is key at the end of the event. Not knowing about this requirement results in wasted time and effort on that aspects of this task that are purely clerical and detract from the more important cybersecurity aspects of TF. While learning aspects of Ghidra, Security Onion, or any other tool would also benefit a TF participant, learning centered on tool use is appropriate during Tracer FIRE – learning about incident response template format does not seem as appropriate.

As the event is meant to mimic forensic incident response tasks that would normally be carried out by a professional in the field, it is suggested that your team chooses a relevant and professional team name and uses presentation tools like a slide show when presenting to the panel.

Help with Heterogeneity

Our university brought 2 females to TF9 and they were the only females out of 27 participants. Racial diversity was somewhat better with seven appearing to be non-white/non-Caucasian. In our current national climate, this is not a novel observation, so we will not dwell on it. We simply encourage more invitations to all student groups.

5. CONCLUSIONS

Cybersecurity has been attracting a lot of attention for the past 20 years and that attention seems to be only intensifying due to the increasing need for cybersecurity professionals ((ISC)2, 2019). Tracer FIRE is a fantastic event for almost any student with interest in cybersecurity – from those new to the field through students with several years of competition under their belts. Though quite mature in its ninth iteration, Tracer FIRE was not known to UNCW CDC members which was a bit surprising given our fairly serious involvement in cyber competitions over the past nine years. We have shared our TF9 experience and reflection to both proliferate the word about Tracer FIRE as a worthwhile exercise and demystify some of its aspects for other future first-time attendees.

6. REFERENCES

Abbott, R.G., McClain, J.T., Anderson, B.R., Nauer, K., Silva, A., & Forsythe, J.C. (2015). Automated Performance Assessment in Cyber Training Exercises.

Anderson, B., Carajal, A., Jarocki, J., McClain, J.T., Nauer, K., Reed, T., Stevens-Adams, S., & Forsythe, C. (2012). Enhanced training for cyber situational awareness in red versus blue team exercises. Technical Report, Sandia National Laboratories.

Carbajal, A., Stevens-Adams, S.M., Silva, A., Nauer, K., Anderson, B.R., & Forsythe, J.C. (2012). Enhanced Training for Cyber Situational Awareness in Red versus Blue Team Exercises.

Childers, N., Boe, B., Cavallaro, L., Cavedon, L., Cova, M., Egele, M., & Vigna, G. (2010). Organizing large scale hacking competitions. In Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 132-152). Springer Berlin Heidelberg.

Fanelli, R.L. & O'Connor, T. (2010). Experiences with practice-focused undergraduate security education. Proceedings of the 3rd Workshop on Cyber Security, Washington, DC.

Hay Group Global. (2012, October 15). *What is experiential learning*? [Video]. YouTube. https://www.youtube.com/watch?v=1ZeAdN4FB5A

(ISC)2. (2019). Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 Cybersecurity Workforce Study, 2019. Retrieved from https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

Kolb, A. Y., & Kolb, D. A. (2013). The Kolb Learning Style Inventory 4.0. Retrieved from https://www.researchgate.net/profile/David_Kolb/publication/303446688_The_Kolb_Learning_Style_Inventory_40_Guide_to_Theory_Psychometrics_Research_Applications/links/57437c4c08ae9f741b3a1a58/The-Kolb-Learning-Style-Inventory-40-Guide-to-Theory-Psychometrics-Research-Applications.pdf

Perry, K.M., Hsieh, G., Butler, C.R., Galvin, Y., & Nauer, K. (2017). Building a Virtual Enterprise Network Environment for APT Experimentation.

Reed, T., Nauer, K., & Silva, A. (2013). Instrumenting Competition-Based Exercises to Evaluate Cyber Defender Situation Awareness. HCI.

Rege, A. (2015). Multidisciplinary experiential learning for holistic cybersecurity education, research and evaluation. USENIX Summit on Gaming, Games, and Gamification in Security Education.

SECCDC. (n.d.). Retrieved from https://cyberinstitute.kennesaw.edu/seccdc/

Security Onion (n.d.). Retrieved from https://securityonion.net/

Security-savvy cyber team proves its 'net worth. (2010, April 16). Retrieved from https://www.llnl.gov/news/security-savvy-cyber-team-proves-its-%E2%80%99net-worth

Siami Namin, A., Aquirre-Muñoz, Z., & Jones, K. (2016). Teaching Cyber Security through Competition an Experience Report about a Participatory Training Workshop. 7th Annual International Conference on Computer Science Education: Innovation & Technology (CSEIT 2016). doi: 10.5176/2251-2195_CSEIT16.39.

Stevens-Adams, S., Carbajal A., Silva A., Nauer K., Anderson B., Reed T., & Forsythe, C. (2013). Enhanced Training for Cyber Situational Awareness. Foundations of Augmented Cognition, Lecture Notes in Computer Science. 8027, 90-99.

Tracer FIRE, Registration Form [Brochure]. (2020).

Treece, A. (Ed.). (2020). Sandia Labs Academic Alliance 2019 Collaboration Report (p. 14, Rep.). Sandia National Laboratories.

Vigna, G., Borgolte, K., Corbetta, J., Doupe, A., Fatantonio, Y., Invernizzi, L., Kirat, D., & Shoshitaishvili, Y. (2014). Ten years of iCTF: The good, the bad, and the ugly. USENIX, Summit on Gaming, Games, and Gamification in Security Education.