From the Campus to the Conference "A Case Study in the Design and Development of Cyber Contests for Professional Conferences"

Brandon Brown
bbrown118@coastline.edu
Computer Service Technology
Coastline College
Fountain Valley, CA 92708, USA

Ronald E Pike
rpike@cpp.edu
Computer Information Systems
Cal Poly Pomona
Pomona, CA 91768, USA

Abstract

Cybersecurity contests and competitions are nothing new. However, most are developed by professional organizations, universities, and industry leading companies. This study looks at the development, design, execution, and ongoing management of one such contest as developed by students for the greater security community at a major Security Conference, DEFCON 26. We will explore practical learning objectives, and how the experience from the classroom, student club, and competition team is harnessed into a well-defined cyber contest that has practicality, educational transportability, and sustainability for future student teams.

Keywords: Cyber Security, Contests, DEFCON, Student Teams, Student Project Management, Cyber Activities.

1. INTRODUCTION

According to the leading security organizations such as the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA), there has only been an increase in the need and demand for cyber security professionals (Oltisk, 2018). This increase is only getting worse and institutions from all sectors are interested in exploring ways to develop these skills quickly and effectively (Oltisk, 2017). One such methodology recently explored was the creation of a unique cyber contest by a group of students for one of the most notable security conferences around, DEFCON. This exercise let the students leverage the skills they learned in the classroom and through competition. The result was a thoughtful and novel contest. It included multiple categories and encompassed multiple areas within cyber security. Finally, it emphasized not only technical skill prowess but required that the students leverage multiple soft and organizational skills to include communication, time, resource, and scheduling management.

Given the issue of a low pool of trained professionals, and an opportunity to provide an experience in a controlled setting, the concept of a multifaceted contest is sound (Cheung, et. Al, 2012). In the case associated with the crafting of the competition for DEFCON, the student team decided to develop a staged or phased approach.

This was constituted of an on-line component for the development of vulnerable applications and platforms. This differs from traditional cyber contests and competitions that typically require participants to run a penetration test, solve a problem, develop a secure application or other typical, repeatable, and accepted methodologies. For the purpose of this writing, there are several groups of individuals that need to be defined. First, the "co-founders" were those individuals who formulated the contest idea and submitted the application to the conference. Next, the "project-team" were those who participated in the design, development, and architecture of the systems that would be leveraged for the contest. This project-team included the co-founders.
Instead, the game creators (student team) outlined a contest where the competitors (cyber security professionals) would complete the preponderance of the work allowing the students to leverage the professionals' technical skills. The premise behind this was to orchestrate a two-phased approach where the first phase was to collect vulnerable images from the primary competitors (cyber security professionals) and that second phase was to showcase these images at DEFCON to the greater security professional audience. This approach allowed the student team to hone design, development, organizational and management skills over an extended period while leveraging the technical skills of the best cyber security professionals in the world.

The easy part of this exercise was the recruitment of the student team. Most campuses, like Cal Poly Pomona, have numerous technology student clubs, cyber competition teams, and a capstone course to bring the talent together in a structured environment. As per Schepens et. Al, (2002) structure in a competitive environment ensures fairness for the participants and ease of administration. This important component is a solid curricular objective within many courses emphasizing ethics, and fairness of play. In this case, the recruitment of students for the initiation of the project was relatively easy. A simple inquiry before a student club meeting generated great interest by a handful of students. After two additional meetings, we were ready to proceed with the application process.

Our next step was to find an appropriate conference to gain the required participation. After selection, we would formulate a plan for the correct alignment of a contest. In our case, this was very easy to do given the time of year and we selected the DEFCON conference slated for August 2018. This selection gave us ample time to plan the contest and communicate with the conference organizers. At the time of our conference consideration, the planning for the DEFCON 2018 conference was in full swing. This conference offered many positive attributes. First, the timing of the application provided a great lead for formation of the contest. Second, the DEFCON contest application process appeared to be very streamlined and offered an excellent fit with this project.

Finally, the location of the conference; Las Vegas, NV, would not be a challenge for travel. After applying, acquiring acceptance from the DEFCON 26 contest board, and tuning our contest concept further, the next step was to build out a larger student team with specialized roles to compartmentalize the work. The logical choice for focusing this effort was to leverage a Senior Project Team in the upcoming Spring 2018 academic quarter. This was fortuitous as the two students who assisted with the initial write-up were eligible or already enrolled in the class.

Once initially formed, the team began the process of researching successful competitions from past DEFCON conferences. Furthermore, the format of the class provided structure and a path for measuring success. Throughout the paper, we will classify these measurements and call out the challenges and ultimate successes of the project to their ultimate fruition of a honed competition format. It is important to note that the success measures and game play methods developed during this project are already making their way into related courses at Cal Poly Pomona.

The ultimate goal of this work is to leverage the information and data gathered through the process of setting up this project for future repetition and expansion into other like areas. With that, we explore the conference selection process, organization of the contest, setup and initial testing prior to deployment to the conference. A subsidiary goal was to ensure that our data collection methodology was sound in order to be successful at the conference. This was key to having the potential for future research work with that data.

2. LITERATURE REVIEW

Cyber contests differ from more traditional competitions from a scope perspective (Fowler, 2017). Contests are shorter in duration than competitions and have a more defined goal whereas competitions are broader, span more technologies and have wider rules set. Contests are more focused on a singular activity concentrate on a specific problem or issue. This can be exemplified by looking at competitions which have multiple contests within them. An excellent example of this is that of the National Cyber League (Tobey, Pusey, and Burley, 2014).

While the majority of the literature in this area has dealt with competitions such as Schepens et. Al, Conklin (2005), White & Williams (2005), Manson et. Al, (2015), and more recently Williams (2018); they do not do a deeper dive into the specifics of contest constructions. This is in contrast with the expansive undertakings that are outlined within many of these articles to the makeup, organization, and logistics to present their competitions. In fact, relative searches through the literature only reveal a handful of references on this typic.

The granular sub-topics of cyber competitions range from Heckman, K. E., & Stech, F. J. (2015), where these authors discuss Cyber Counter deception to Schmidt et. Al (2015), where the authors examine links between similar cyber issues and challenges in the private and military sectors. Nowhere in the literature were contest organization, building, examples, and challenges found. This topic has not been studied at any length.

3. CONFERENCE SELECTION

As mentioned previously, the logical choice for a conference was the DEFCON 26 conference in Las Vegas. This conference, held in late July or early August, provided enough lead time for formation of concept, design, and planning. Additionally, the application process was streamlined and aligned with our term for the academic year. Other conferences considered were Layer One, Los Angeles; ToorCon, San Diego; Black Hat USA, Las Vegas; and SCALE, Los Angeles. These conferences were considered given their relative location of our campus, relevance of contest topic, and maturity of event. However, DEFCON offered not only the best timing for our project but also the largest group of cyber security professional's as participants.

In addition to the conference considerations, the team examined the potential of hosting the contest at a smaller gathering. Potential candidates were campus oriented such as technology club symposiums. This would have provided further development in the case that our application with one or all of the conferences were not accepted. As it turned out, the DEFCON 26 conference significantly expanded their contest, workshop and village program for this year and this project was well received. We believe this research is easily replicated as in any geography there are ample cyber security conferences to select from across North America. According to InfoSec, there are over seventeen hundred events listed for 2018. With so many to choose from, even startup organizations have a better than average chance to obtain a venue for their security contest.

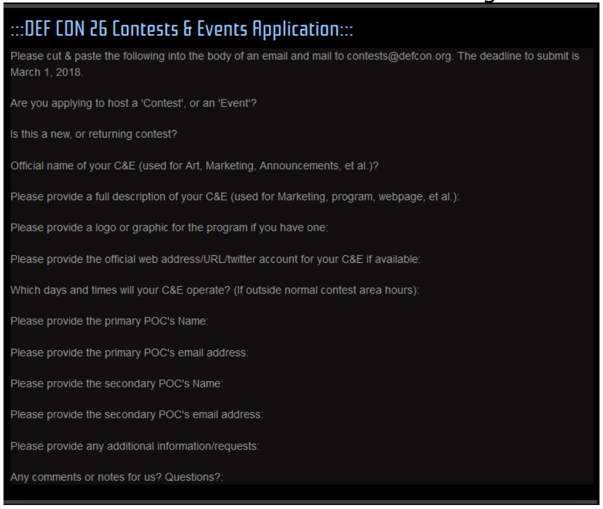
4. DEFINING THE CONTEST

At the beginning of this process, the co-founders brainstormed a broad concept for a contest. We examined the existing and past contests at several of these conferences from archive material readily available from several of their websites. Several patterns were immediately prevalent. Of these, multiple "capture the flag" and "force on force" contests persist and are well established. However, there was one evident gap. In our case, this gap took on the idea of creating a contest for the creation of a contest. The proverbial "Russian Doll" if you will. (meta-competition?)

Many conferences align to specific types or topics for contests in the same way that academic journals provide guidelines for calls for papers. This criterion is typically found on the conference web site. One good example is that of ShellCON L.A. This conference is much less mature than DEFCON but has an advantage of being open to new ideas and not afraid to take on novel initiatives such as the contest we were designing. However, they still had guidelines for papers, workshops, and contests that aligned to the topics and themes within cyber security that they were exploring. In this way, the conferences provide guidance in a similar way as academic journals do for submission of papers.

After outlining the contest and conceptualizing a design; the co-founders decided to structure our contest around the creation of vulnerable images that could be judged by the public at the conference in an "Open Sandbox" format. In addition to hosting the images, we, the contest organizers, would develop the systems to accept, house, and preview submissions. Once this idea was firmly on paper, we began approaching the idea of submitting the contest topic and outline to different conferences.

Our first choice was DEFCON 26. At the time of submission, DEFCON 26 had an open call for papers, workshops, contests etc. DEFCON called this their "Call for Everything". The process was relatively simple and much like the submission for academic papers to conferences. They provided guidelines, format, and deadlines. All submissions had to follow the format as seen in Image 1.



:::DEF CON 26 Contests & Events Application:::

Please cut & paste the following into the body of an email and mail to contests@defcon.org. The deadline to submit is March 1, 2018.

Are you applying to host a 'Contest', or an 'Event'?

Is this a new, or returning contest?

Official name of your C&E (used for Art, Marketing, Announcements, et al.)?

Please provide a full description of your C&E (used for Marketing, program, webpage, et al.):

Please provide a logo or graphic for the program if you have one:

Please provide the official web address/URL/twitter account for your C&E if available:

Which days and times will your C&E operate? (If outside normal contest area hours):

Please provide the primary POC's Name:

Please provide the primary POC's email address:

Please provide the secondary POC's Name:

Please provide the secondary POC's email address:

Please provide any additional information/requests:

Any comments or notes for us? Questions?:

Image 1 – DEFCON Event Application

Our application was straight forward and all submissions were done via e-mail.

The original submission criteria for the Vulnsec contest with answers included:

:::DEF CON 26 Contests & Events Application:::
Please cut & paste the following into the body of an email and mail to contests@defcon.org. The deadline to submit is March 1, 2018.

Are you applying to host a 'Contest', or an 'Event'? – Contest

Is this a new, or returning contest?

New - Brand New. Cool New! Did I say NEW!!!

Official name of your C&E (used for Art, Marketing, Announcements, et al.)?

VulSec Vulnerable Image Building Contest
Please provide a full description of your C&E (used for Marketing, program, web-page, et al.):

The "VulnSec" Vulnerable Image Building contest is an event that breaks the traditional mold of DEFCON contests / conquests. Instead of a contest based around hacking into an environment, this is a contest based on making that environment to be hacked and being judged by different criteria (Ease of Use, Creative Environment, Practicality, etc...). Each contestant must submit a VM for their category No Later Than Friday Noon of DEFCON! All day Saturday will be dedicated to having DEFCON participants take the VMs through their paces and fill out a scoring Card / form for any VM they work with. Scoring Criteria will be levied based on participation (Number of Users attempting the VM) and the user's critique from provided scoring cards. At this time, there are a few sponsors (individuals and companies) that will provide simple, (Not too expensive) prizes for the winners of all categories.

VulnSec will provide an on-site "Cyber Range" for this contest for upload of VMs. VulnSec will support both VMware and VirtualBox VMs.
All VMs will be "Standalone" and not require back-end / cloud support. VulnSec will provide networking equipment and if needed, Kali Linux VMs for hackers to test out the contestant VMs.
This should be an exciting event for ALL DEFCON attendees whom can spend as much or as little time as they like. VulnSec will provide on-site marketing materials and flyers to promote their event in addition to DEFCON marketing / advertisements.

Contest Outline & Image Criteria:

Linux & Windows
Kids Beginner (18 & Under)
Kids Advanced (18 & Under)
Novice
Intermediate
Advanced
Judging Criteria:
Ease / Difficulty of Overall Hack
Known OS / App vulnerabilities
Remote Code Execution vs. Local Priv.
Web Content Vulnerabilities
Crypto / Puzzle
Use of appropriate level of content
# of Vulnerabilities
Creative “Hackiness”
Background Scenario
Environment
Humor etc...
Requirements, Rules & Limitations:
Contestants MUST provide a 1 Paragraph "Write Up" of their Image (Under 300 Words!)
This will be "Advertised" at the Table for Player/Judges to sift through.
Size of VM must be under 40GB for Windows & 15 GB for Linux
All VMs must be rated PG!!!! ONLY!!!!

Scoring will be based on a 100 point scale broken down by criteria and requirements per score cards. Thus, the more scorecards your VM obtains, the more points you will be awarded!

General Guidance for Participants:

VMs in the Beginner Categories should be "Script Kiddie Friendly" so as to motivate beginner hackers to the table.

VMs in the Intermediate Category look to have more advanced vulnerabilities not necessarily identified by automated scanners

VMs in the Advanced Category should require hackers to exploit custom buffer overflows, unidentified services, and incorporate fuzzing as a premise.

Please provide a logo or graphic for the program if you have one:

Original Logo Provided:

Image – 2 – Original Vulnsec Logo

Please provide the official web address / URL / twitter account for your C&E if available:

http://vulnsec.net

Which days and times will your C&E operate? (If outside normal contest area hours):

Normal Contest Hours of DEFCON

Please provide the primary POC's Name:

Brandon Brown

Please provide the primary POC's email address:

brbrown@cpp.edu

Please provide the secondary POC's Name:

Jonathan Maxwell

Please provide the secondary POC's email address:

p4tches@protonmail.com

Please provide any additional information / requests:

Internet Connection. A 20x20 foot space (Or as Big as you can give us!) 6 110 Electrical Outlets. Additional Questions asked of DEFCON:

Does DEFCON provide Human or "Other" Badges for accepted Contest Organizers?
If so, what would be the limit.

This was to inquire about number of students / staff we could p[potentially stipend.

We only had a few questions regarding the DEFCON conference as the co-organizers had attended the conference many times in the past. The only item we were lacking up front was an actual website. This gap would be the premise to the remainder of the project as it would serve as the springboard for the development of many aspects of the contest.

5. REFINING THE FOCUS AND VISION OF THE CONTEST

Acceptance to the DEFCON 26 conference took about three weeks and there was some back and forth between the co-founders and the organizers of the DEFCON 26 contests. After acceptance, the co-founders quickly approached other faculty to help with the development of the contest. It was decided to use the opportunity of a Senior Project course to facilitate the development of the contest.

This is conceptualized in Kolychev and Prokhorov (2015) where they give a premise to the concept of effectuation in the development and execution of projects. This is especially useful in student project teams where there is limited project management skill and the focus is on learning these skills while meeting external goals. Our team came together quickly given the news of the co-founders' acceptance of the contest to DEFCON 26. A team of seven (7) were selected which included the co-founders.
After formation, the hard work started. This included a more defined set of rules, marketing plan, and technical specifications. The latter included sub categories for image acceptance,

validation, and storage. Further refinement of the contest project was split between project team members and a student project manager was put in charge. The Senior Project course would run for eleven weeks giving the student project team ample time to meet the requirements and deliverables of the project. The result was a refined project with clearly stated objectives to be executed for the DEFCON 26 contest in August 2018.

6. SETUP AND INITIAL EXECUTION (TESTING) PHASE

Once formed, the project team quickly put together a plan to delegate the work and compartmentalize their efforts. The assigned student project manager did a good job in establishing a communication plan. Finally, faculty provided oversight and guidance. The result was a project that was delivered on-time, within scope, and on budget. These three factors were achieved through solid project management principles using Agile guidelines (Highsmith, 2009).

The project did offer challenges such as the system needing to accept, validate, categorize, and store the images being submitted for the contest. The fact that the images were submitted by clever cyber-security professionals meant the primary challenge was accepting images and storing them in a secure manner. Also, a registration link needed to be created that teamed up with the image. It was decided to follow a decentralized model. This model is outlined in Haeberlen et. Al. (2005). This methodology provided resiliency and redundancy to mitigate the risk of loss of data.

A fully developed project plan helped with the framing of the necessary steps to meet the deliverables as set out by the co-founders. These deliverables aligned with the contest criteria outlined previously. In addition, some changes were made to the contest to enhance inclusiveness in the activity. This included the formulation of a schedule to highlight the different categories throughout the conference, the formation of special "time trials" to pose challenges to participants regardless of level of experience, and an open "cyber range" time where conference goers could merely walk up, interact, and participate ad hoc. As these items were being adapted, the nature of the contest took shape and changed somewhat to where the team noticed the two differential perspectives of the contest take shape. This was not too unexpected as development of these types of contests have seen similar evolutions as outlined by Storn (1996).

Finally, a few designs were conceptualized for the purpose of administration of the contest as well as ease of traffic control for participants. DEFCON held a call about three months before the conference to go over guidelines, answer questions, and provide pertinent information regarding the contest area. Prior to this call, the team was requested to provide a diagram for the planning of the contest area. Given we were submitting for a new contest and had limited experience with this level of competition design, we leaned on collective experience and guidance. In this situation, we looked to Estes et. Al. who surmised many existing practices of prior works (Estes, et. Al, 2016).

Image three (3) shows the proposed layout that was approved by the DEFCON contest organizers.

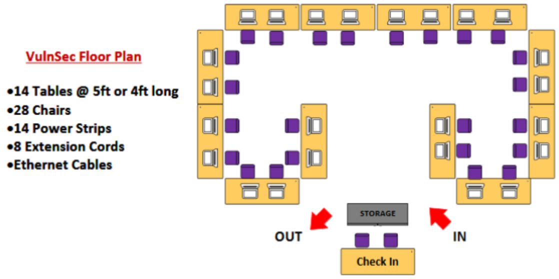


Image 3 – Proposed Setup and Seating Chart

This image shows a 25 X 20-foot area encompassing two workstations per table for a total of 24. Furthermore, an initial schedule was adopted for the contest as outlined:

-----DEFCON 26-----
Vulnsec Contest
Vulnerable Image Contest
Schedule: Aug. 8 – 11

Thursday:
Setup
QA & Test.
Selective Invites

Friday:
10AM – Event 1 – Intermediate Image #1 & #2
11AM – Event 2 – Advanced Image #1 & #2
12PM – Event 3 – N00b Image #1 & #2
1PM – Event 4 – R00Tz Beginner Image #1 & #2
2PM – Event 5 – R00Tz Intermediate Image #1 & #2
3PM – Event 6 – Special Event Time Trial!
4PM – Event 7 – R00Tz Beginner Image #3 & #4

5PM – Event 8 – R00Tz Intermediate Image #3 & #4
6PM – Event 9 – N00b Image #3 & #4
7PM – Event 10 – Advanced Image #3 & #4
8PM – Event 11 – Intermediate Image #3 & #4

Saturday:
10AM – Event 1 – Workshop on Constructing Web Vulnerabilities
11AM – Event 2 – Advanced Image Consolation
12PM – Event 3 – Workshop on Constructing Network Vulnerabilities
1PM – Event 4 – Intermediate Image Consolation
2PM – Event 5 – R00Tz Intermediate Image Consolation
3PM – Event 6 – Special Event Time Trial!
4PM – Event 7 – Workshop on Flag Implants & Activities
5PM – Event 8 – R00Tz Beginner Consolation
6PM – Event 9 – N00b Image Consolation
7PM – Event 10 – Open Cyber Range – Pick your Image
8PM – Event 11 – Open Cyber Range – Pick your Image

Sunday:
10AM – Event 1 – R00Tz Beginner Final
11AM – Event 2 – N00b Image Final
12PM – Event 3 – Intermediate Image Final
1PM – Event 4 – Advanced Image Final
2PM – Event 5 – Special Event & Awards

7. STUDENT ENGAGEMENT

Student engagement throughout the steps of setting up the contest was enthusiastic and sustained. Qualitative feedback from the student participants reflected this and only one meeting over the course of the eleven-week quarter was postponed. No meetings, work sessions, or collaboration efforts were missed by any student. This was recorded by attendance rosters for team meetings and were submitted to the faculty organizers at the end of the term. Impromptu inquiry throughout the term addressed this phenomenon. It was found that the level of student enthusiasm was greatly elevated by the topic of the project. The general question or solicitation of information was regarding the student's individual enthusiasm regarding the project. The resounding response to these inquiries were met with the statement"
"It's DEFCON!"

This reaction sufficed to say was the driving factor. The students by the time of the project start had secured admittance to DEFCON 26 and therefore progressed with the attitude of a highly motivated team. This was reflected in their work, communication, and interaction with faculty and one another.

Keep in mind that the DEFCON conference was not the first security conference but it is the largest and one of the most prestigious in the world. The commonality and general availability of security conferences are well known. However, none have the luster and persona of DEFCON. Given this, the motivation of the students was greatly impacted in a positive way and their work reflected this.

8. FOLLOW UP RESEARCH

At the time of this writing, the contest is not underway. This gives an incomplete picture to the ultimate success of the endeavor. Furthermore, there are multiple opportunities to take advantage from this project for a research perspective. These include but are not limited to:

- Data Collection on Attack methodologies
- Identification of common vulnerabilities
- Identification of unique vulnerabilities
- Identification of common hacking tools
- Identification of uncommon or non-used tools

The latter is subjective in terms that the researchers can isolate not only what tools were used but also what tools and techniques were not used. This provides the researchers a better insight in how to craft activities and teaching opportunities to incorporate into the classroom. Finally, this will lead to the incorporation of alignment to common certification programs such as the Certified Ethical Hacker, Offensive Security Certified Practitioner, and Offensive Security Exploitation Expert.

9. INITIAL FINDINGS FROM THE DATA

At the time of submission, the team was able to collect roughly three hundred (300) gigabytes of data from PCAP files. Initial analysis of this data shows the different tools that the participates of the contest used in attempting to breach the vulnerable images. Although these files have not been parsed and dissected from a forensic standpoint, the initial pass of packet types, applications fingerprints, and error transmissions shows trends of common tools between participants. This included use of common applications such as NMAP, NetCat, the Metasploit Framework, and simple browsers.
A more in-depth analysis is intended and this data will be made freely available at some point in the future.

10. REFERENCES

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012, January). Effectiveness of cybersecurity competitions. In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Conklin, A. (2005, September). The use of a collegiate cyber defense competition in information security education. In Proceedings of the 2nd annual conference on Information security curriculum development (pp. 16-18). ACM.

Conti, G., Babbitt, T., & Nelson, J. (2011). Hacking competitions and their untapped potential for security education. IEEE Security & Privacy, 9(3), 56-59.

Dutta, S., & Mathur, R. (2012, March). Cybersecurity—An integral part of STEM. In Integrated STEM Education Conference (ISEC), 2012 IEEE 2nd (pp. 1-4). IEEE.

Estes, T., Finocchiaro, J., Blair, J., Robison, J., Dalme, J., Emana, M., ... & Sobiesk, E. (2016, September). A Capstone Design Project for Teaching Cybersecurity to Non-technical Users. In Proceedings of the 17th Annual Conference on Information Technology Education (pp. 142-147). ACM.

Haeberlen, A., Mislove, A., & Druschel, P. (2005, May). Glacier: Highly durable, decentralized storage despite massive correlated failures. In Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2 (pp. 143-158). USENIX Association.

Highsmith, J. R. (2009). Agile project management: creating innovative products. Pearson education.

Kolychev, V. D., & Prokhorov, I. V. (2015). Conception, technology and methods of development of university system of innovation projects commercialization based on effectuation. Asian Social Science, 11(8), 44.

Manson, D., Pusey, P., Hufe, M. J., Jones, J., Likarish, D., Pittman, J., & Tobey, D. (2015, June). The cybersecurity competition federation. In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (pp. 109-112). ACM.

NAFIPS., 1996 Biennial Conference of the North American (pp. 519-523). IEEE.

Oltisk, Jon (2018, Jan. 11) Research suggests cybersecurity skills shortage is getting worse. *CSO* Retrieved from: https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html.

Oltisk, Jon (2017, Aug. 10) How to address the cybersecurity analytics and operations skills shortage *CSO* Retrieved from: https://www.csoonline.com/article/3215090/security/cybersecurity-analytics-and-operations-skills-shortage.html

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. IEEE Security & Privacy, 10(3), 76-79.

Sommestad, T., & Hallberg, J. (2012, October). Cyber security exercises and competitions as a platform for cyber security experiments. In Nordic Conference on Secure IT Systems (pp. 47-60). Springer, Berlin, Heidelberg.

Storn, R. (1996, June). On the usage of differential evolution for function optimization. In Fuzzy Information Processing Society, 1996.

Wayne Schepens, Daniel Ragsdale, John Surdu, The Cyber Defence Exercise: An Evaluation of the Effectiveness of Information Assurance Education, The Journal of Information Security, Volume 1, Number 2. July, 2002

White, G. B., & Williams, D. (2005, October). The collegiate cyber defense competition. In Proceedings of the 9th Colloquium for Information Systems Security Education.