Cybersecurity Competitions as Effective Cybersecurity Teaching Tools

Yoshuam A. Alicea
Polytechnic University of Puerto Rico
Electrical & Computer and
Computer Science Department
San Juan, Puerto Rico 00918
Email: yoshuamalicea@gmail.com

***Abstract** – For some time researchers have been studying how to attract students to the Cybersecurity field due to the shortage that currently exists. To address this issue, they have been modifying curriculums, developing programs and using cyber competitions in order to attract students to study this important field. Cybersecurity competitions have been very effective, but a few question still need to be answered: How much does the student improve after participating in these competitions? What can we use from the cyber competitions to apply to the classroom so students can be attracted to, and better prepared for, this field?*

I. Introduction

For some time, the Cybersecurity field has been experiencing a shortage of computer security specialists in the U.S. This problem is being addressed by some entities, like the National Science Foundation (NSF), Cyber Corps and many others, that are funding students who wants to pursue a career in the computer security field [3]. Also, many universities have been developing curriculums based on that need in order to fill the gap that is continuously growing in the Cybersecurity field. One of the struggles universities have is how to effectively teach computer security concepts so students can be competitive once they start performing as security professionals in a working environment. To speed up the learning process in an effective way, students must have a hands-on experience where they can apply the knowledge acquired in the classroom.

Time can be very limiting while teaching security concepts because sometimes the student needs more practice in certain areas that they find difficult. Class laboratories sometimes are not effective in filling in those gaps. Also, some students are not that committed in their classes because they find them boring, superficial, or not challenging at all. For this reason, we need to develop other activities that help to keep students engaged with the learning process, and encourage them to keep on learning. One way to accomplish this goal is making students participate in Cybersecurity competitions.

Cybersecurity competitions such as “Capture the Flag” (CTF) are a type of event where students from the same or different universities apply their knowledge against others to solve computer security related problems. At the same time, they also learn more about how hackers are able to get into computers and how to defend against them.

A really effective attribute that CTFs have is that every student involved needs to research about some topic in order to solve the challenges. By doing this, they are strengthening their ‘self-learning’ skills and at the same time they are learning cybersecurity concepts like reverse engineering, cryptography, computer forensics, steganography, programming, system administration, network security, web security, enumeration, and social engineering, among others. Furthermore, the CTF competitions allow students to work as a team, giving the student the ability of choosing a subject of expertise and joining other students with different areas of expertise, and working together as in a real working environment. The importance of this aspect is learning that teamwork is always needed in order to be successful.

Another interesting fact is that when competitions end students share their knowledge on how they worked out the solution for the different challenges by documenting the method they applied to solve the task. This allows newcomers in the computer security field to learn more about the tools or “methods” used to solve the everyday challenges. This helps cybersecurity professionals in two ways. First, the student that makes the write up will be challenged intellectually at the time of writing the explanation of how he solved the challenge. This means, that if the student explains the solution with ease and good understanding on the topic, they receive a self-feedback on how their knowledge has increased. Second, the student that couldn't solve a challenge can read another student's write up and learn how to approach similar problems in the future. This means that he'll be setting on a path to acquire the required knowledge for a specific topic. Knowing these two factors, the author decides to test those competitions in a classroom. A group of six students with interest in the cybersecurity field but inexperienced were exposed to a format similar to a CTF competition in an undergraduate course in Penetration Testing to see how much their knowledge would increase in three months.

The course and CTF activities were organized and delivered by the Author, Dr. Jeff Duffany (professor and security specialist), and PUPR NSF-SFS Fellow Steven Bennet. Also, another six students that are NSF-SFS scholars/fellows with experience (that were part of the PUPR CTF Team called *1nc0gnito*) were selected, to compare the results from the inexperienced students vs. these experienced students.

II. Methodology and Tools

The two set of students (inexperienced and experienced) were subject to the same tests except that no training was given to the experienced set of students.

This research was divided into three phases:

- Phase 1 – The six inexperienced students were exposed to the developed course curriculum.
- Phase 2 – Both, the inexperienced and experienced, students competed in three games provided by the National Cyber League Competition (NCL) [1]. Two of the games tested the students as individuals, and one as a team.
- Phase 3 – The data gathered from the scouting reports provided by the NCL for individual and team games was analyzed. The following steps were followed for the analysis:
    1. For the first two games: The completion percentage and accuracy of the inexperienced students with the completion and accuracy of the experience students was compared. To do this more effectively students were matched with their performance so the inexperienced student with best performance could be compared with the experienced student with best performance, and so on. Then, the difference between them was calculated to obtain the performance of the inexperienced students using the experienced student as a control.
    2. For the team based games: The categories of the competition were considered, comparing how well the inexperienced students did, compared to the experienced students. With this analysis, the strengths and weakness of the inexperienced team could be observed. Recommendations will allow more modifications to the curriculum, making it more effective.

National Cyber League (NCL) How it works?

The NCL is a national competition that is held two times in the year, one in the Spring season and the other in the Fall. It provides an ongoing virtual training ground for participants to develop, practice, and validate their cybersecurity knowledge and skills. The good thing of NCL is that it provides a 'gymnasium' for the participant to train and learn skills before, during and after the competition.

This competition ranks their players by points and accuracy. This means that all attempts are taken into account at the time of ranking players. This ranking method allow the participants to analyze more carefully their solution and allows them to focus on the problem to gain a better understanding of it. This game is easier than the other two games.

Each season of the NCL is divided into three games:

- Preseason – This game tests every participant as an individual. The goal of this game is to place the student within the Gold, Silver or Bronze brackets.
    - Gold Bracket – (Experienced Players) participants ranked in the top 15% position

    - Silver Bracket – (intermediate players) participants ranked in the Next 35% positions
    - Bronze bracket – (novice players) participants ranked in the remaining 50% positions
- Regular Season – This game is more advanced and players compete individually. This time the players compete in their qualifying bracket.
- Postseason – This is the most challenging game because players compete as a team with a maximum of 10 players. Here the challenges are harder and the accuracy is shared within the player.

The NCL test the students in the following areas:

- Open Source Intelligence (OSINT)
- Scanning
- Password Cracking
- Cryptography and Steganography
- Analysis
    - Network
    - Log
- Exploitation
    - Web
    - Wireless Access
    - Binary (Reversing)

A syllabus including the CTF concepts was prepared for the students in the Penetration Testing course based on the above-mentioned Cybersecurity topics.

The Curriculum

To give students the flavor of the CTF competition in the Penetration Testing course, wargames that are freely available on the internet were used for everyone interesting in learning cybersecurity. The curriculum was divided using the topics/categories that NCL uses in their competition as follows:

- Cryptography and Steganography – For this category students were given a hands-on exercise where they needed to identify the encoding scheme or cipher and apply different techniques, like brute force attack, known-plaintext attack, partial key attack and dictionary attacks. Also, a hands-on exercise on RSA encryption exploiting the *low N vulnerability* was given to students.

  On the topic of steganography, students were trained to use steghide and stegui for performing steganography inside pictures and audio. Also, they were taught of the least significant bit method for steganography.
- Log Analysis – For this category the bandit challenge in *Overthewire.org* website [2] was used. The reason for choosing this wargame was because it provides an environment that is easier for the novice, and also teaches Linux shell commands that are very useful for parsing data, like a Log using command line tools. Also, it teaches Secure Shell connection which is a plus for the student.
- Password Cracking – For this category students received some training on how to use hashes for data integrity. Also, training was given on using tools like *john the ripper*, *ophcrack* and how to build their own dictionaries for password cracking.
- Network Analysis and Wireless Access – For these two categories students were trained using *Wireshark* for analyzing the captured traffic. Also, how to extract information from the captured packets, follow the tcp stream, filter packets by ip address, identify protocols and how to analyze wireless traffic.
  For the Wireless Access category students were trained to use *aircrack-ng* to identify the protection of the packet and then how to use that tool to crack the network password.
- Web Exploitation – For this category the *Natas* challenge of the overthewire.org site was used. Using this challenge, students were able to learn from basic google hacks to SQL injections. They were trained to tamper data, perform cross site scripting attacks and perform cross site request forgery. They were taught the basics of *JavaScript* obfuscation techniques and how to use the developer's tool for their advantages.
- Scanning – For this category students were taught how to use the *nmap* tool for ip scanning and *dirBuster* for endpoint scanning. Finally, *wpscan* for WordPress application scanning was covered.

- Binary Reverse Engineering – For this category the students were taught how to use *GNU Debugger* (*gdb*) for debugging binary executables. Also, they were taught how to use some tools like strings. Even though NCL did not go deeper on shell coding a class was given on how shellcodes work and how to use them to exploit programs using a buffer overflow vulnerable executable as example.

- Open Source Intelligence – For this category students were trained on how to look for information over the Internet using the search engines features for effectively obtaining expected results.

III. Analysis

NCL Preseason game

The Preseason game was easier than the other two because its purpose is to qualify students in their respective brackets. It tests in four (4) categories: Open Source Intelligence, Cryptography, Network Analysis and Log Analysis.

It was expected that the control group (experienced set of students) would make it to the gold bracket, while the inexperienced group would make it to the bronze bracket. But, for our surprise, the inexperienced group made it to the Silver bracket and only one student made it to the bronze bracket. So, they performed better than expected.

After analyzing the data gathered from the Scouting Report of the NCL (of both sets of students) it could be observed that the difference between students on game task completion were very consistent for both experienced and inexperienced students.

In Figures one (1) to four (4) the *x* axis represents the set of participants from each of the teams. The *y* axis represents the percentage or 'difference' of accuracy between the experienced student and the inexperienced student.

The top of the bar represents the experienced student and the bottom of the bar represents the inexperienced student. Percentage of accuracy for each set of students from each team is observed in the bar chart.

The margin of difference between the inexperienced students ranged from 30.3% for the least performance student down to 8.6% for the best performance student, which is very good for the inexperienced students (see Figure 1).

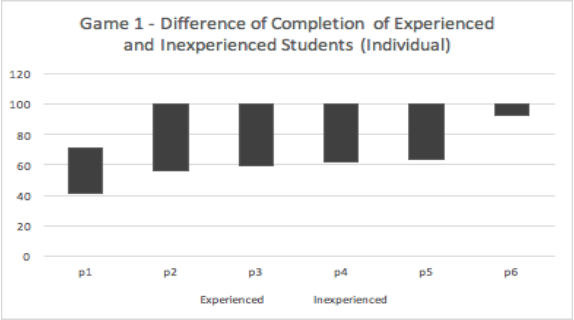

Figure 1 – Difference in completion between Experienced (top of the bars) vs. Inexperienced (bottom of the bars) students.

Even though the inexperienced students could not finish all the tasks they were able to solve a great percentage of them which means the topics of the course were, in general, very effective.

In order to study how accurate the inexperienced students' performance was during the completion of the Preseason game, we used the accuracy reported by the NCL, which presents the attempts made, versus the correct answers.

After analyzing the difference between the accuracy of each set of students, it could be observed that the inexperienced students were close to the experienced team. The farthest difference was 35% and the closest one had an 18% difference (see Figure 2). This result was good for the inexperienced students, since the accuracy reveals how careful they were at the time of solving the tasks.

Using the previous two analysis, it was determined that the students performed well in the first game which was the easiest one.

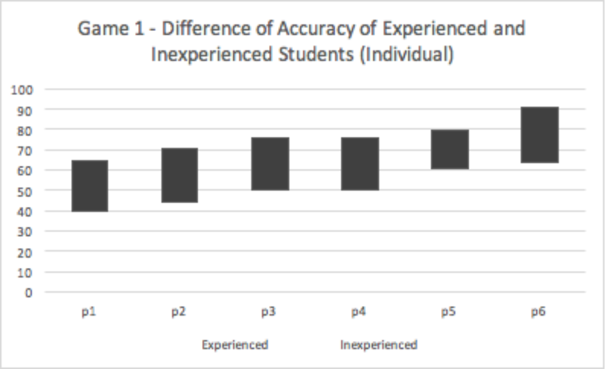

Figure 2 – Difference in accuracy between Experienced (top of the bars) vs. Inexperienced (bottom of the bars) students.

NCL Regular game

This game was held after students were placed into their qualifying brackets. In this game, the students were evaluated in more categories than the Preseason game. The categories added are: password cracking, web application exploitation, wireless access exploitation, enumeration and exploitation (Reverse engineering) and scanning. This game's difficulty level increased substantially compared to the Preseason game.

After analyzing the data gathered from the scouting report of the NCL (of both student sets on game task completion), the performance of the inexperienced students was low (see Figure 3). According to the data gathered the margin of difference of the least performing student ranged from 46.7% down to 19.2% for the best performing student. This time the inexperienced students dropped by approximately 10% from their previous completion evaluation. However, as inexperienced students they did a good job. Also, the result of this analysis reveals that some parts of the curriculum (related to the newly added categories) needs to be hardened in some areas to teach students more analysis techniques and how to apply them to difficult problems.

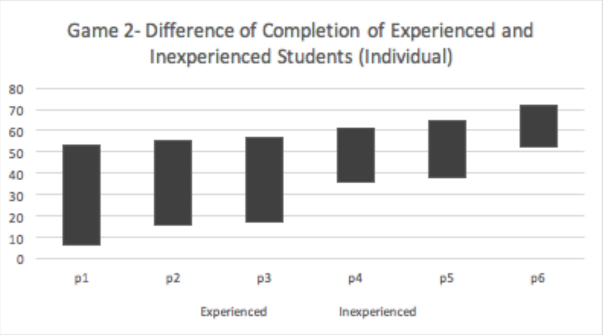

Figure 3 – Difference in completion between Experienced (top of the bars) vs. Inexperienced (bottom of the bars) students.

For the accuracy analysis of both set of students the results for the inexperienced students were similar to their previous game even though they dropped a little (see Figure 4).

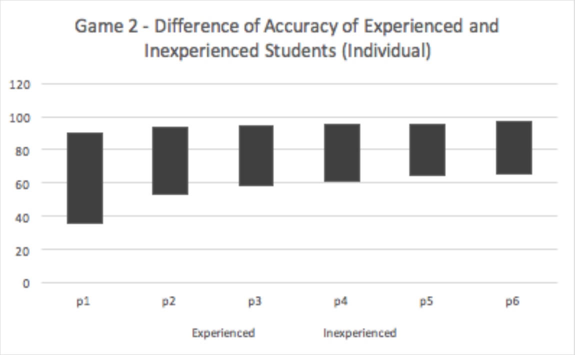

Figure 4 – Difference in accuracy between Experienced (top of the bars) vs. Inexperienced (bottom of the bars) students.

According to the scouting report provided by the NCL the farthest difference against the experienced students was 54.2% and the closest difference was 31.2%. This time it was observed that the experienced students were more focused since they increased substantially their accuracy, but the inexperienced students maintained their accuracy. The inexperienced students had to struggle a little because of the difficulty of this game. This problem could be addressed in the future by increasing the hours of training for inexperienced students.

NCL Postseason game (Team based)

For this game a different approach is taken in the analysis. Each performance is compared by category studying each teams' execution (inexperienced students compared to experienced students).

According to the scouting report provided by the NCL the inexperienced students did really good in open source intelligence, cryptography and password cracking, but they were very weak at log analysis, network analysis, wireless access exploitation, scanning, enumeration and exploitation and web application exploitation (see Figure 5). The experienced team was also weak at web application exploitation but in the other areas they were consistent, so they were neither outstandingly strong, or weak. After this analysis of completion, it was understood that there was a need to enforce the curriculum in the areas where performance was weak, as mentioned above, in order for the inexperienced students to be more effective in the future.

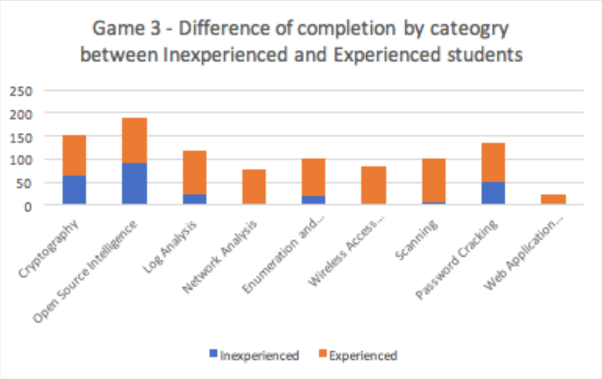

Figure 5 – Difference in completion by category between Experienced (orange) and Inexperienced (blue) students.

The other analysis performed in this game was the comparison between the accuracy of each category of the inexperienced students versus the accuracy of each category of the experienced students.

After analyzing the scouting report provided by the NCL it could be observed that each team maintained a good accuracy in this game (see Figure 6). This could be associated to good teamwork in both parties. After this analysis, it was decided to add a teamwork based CTF activity into the curriculum because each student can also be trained by their strongest members to learn faster.

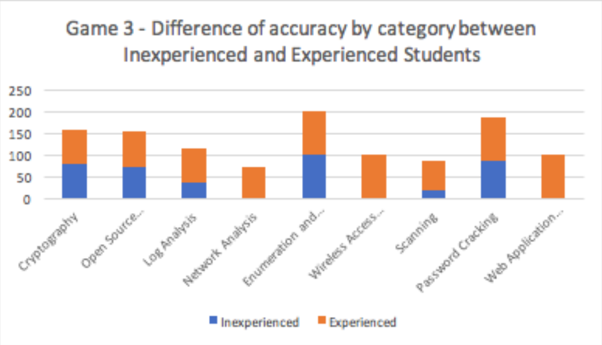

Figure 6 – Difference in accuracy by category between Experienced (orange) and Inexperienced (blue) students.

IV. Conclusion

After analyzing the results, it is concluded that the curriculum needs more modifications to be effective in teaching students the cybersecurity concepts.

For the inexperienced students, it could be observed that there were certain areas that were easier for them to learn using the CTF activities in the course. These areas were cryptography, open source intelligence, and password cracking. So, using CTF in Penetration Testing courses can quickly improve the skills of students in those areas. More emphasis is needed in areas such as: network analysis, wireless access exploitation and enumeration and exploitation (reverse engineering). These were the weakest delivered components in the course. Also, new techniques need to be taught to provide students and security professionals easier approaches to more complex problems.

Other studies can be done using different competitions such as the Collegiate Cyber Defense Competition (CCDC) [4]. This competition tests the students in a real-world environment, where instead of attacking a system they have to defend it. Using competitions like CCDC test how students work in stressful situations and how they can manage that stress as a team. They share techniques and train to manage these types of situations in an effective manner.

Finally, after analyzing the data gathered from the NCL scouting reports, it was observed that teamwork is very effective to achieve an effective cybersecurity career. Both the experienced and inexperienced students performed better as a team than as individuals. Including CTF competitions focused on teamwork in the curriculum is a topic for future research.

V. References

[1] About NCL. (n.d.). Retrieved May 17, 2017, https://www.nationalcyberleague.org/about

[2] Wargames. (n.d.). Retrieved May 18, 2017, from http://overthewire.org/wargames/

[3] Cobb, S. (2016). Mind This Gap: Criminal Hacking and the Global Cybersecurity Skills Shortage, a Critical Analysis. Retrieved from https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cobb.pdf.

[4] National Collegiate Cyber Defense Competition. (n.d.). Retrieved May 19, 2017, from http://www.nationalccdc.org/