Capture the Flag: Website Tutorial to Boost Cybersecurity Training

Author: Reinaldo E. Santiago Lozada
Advisor: Dr. Jeffrey Duffany
Electrical & Computer Engineering and Computer Science Department

Abstract

Cybersecurity is a new topic in many organizations, including educational organizations. This new field will have an increase, as new technologies emerged. For that reasons, in order to meet the cybersecurity personnel demand, it is vital to boost cybersecurity interest among students and workers. There are new ways to participate and get involve with this new field, which is the Capture the Flag Competitions. Capture the Flag (CTF) competitions permit students and workers to learn cybersecurity skills in a different and interesting approach. These competitions are platforms that keep them interested in cybersecurity and prepare them for defensive against real cyber attackers.

Introduction

This project will focus on developing a web page for tutoring people on Capture the Flag competitions (CTF). These competitions distill major disciplines of professional computer security work into short, objectively measurable exercises. The primary goals and objectives for this project are as follow:

- Get students familiarize with cybersecurity concepts, so they incite the interest in cybersecurity.
- Students knowledge about CTF and general cybersecurity competitions increase.
- Students confidence and comfort level increase as they participated in real CTFs.

Background

Cybersecurity is a high priority of companies, small and big, as cyber-attacks have been on the rise in recent years. In response to these attacks, security professionals and college students have been through rigorous training as how hackers are able to get into the companies and how to defend against them. One way of cyber security training is through a cyber security capture the flag (CTF) event. A cyber security CTF is a competition between security professionals and/or students learning about cyber security. This competition is used as a learning tool for everyone that is interested in cyber security and it can help sharpen the tools they have learned during their training and classes.

Problem

Capture the Flag (CTF) competitions, allow students to learn cybersecurity skills in a fun and engaging way. CTF competitions are effective platforms to increase student interest in cybersecurity and prepare them for defending against real cyber attackers [7, 8, 9]. The game-like environment of CTF competitions engage students in solving complex cyber-challenges. With proper training and preparation, such competitions can produce high quality cybersecurity professionals [7, 10]. For that reason, which are the areas that students needs to know to compete in this competitions, and which are frequently seem on this competitions?

Methodology

The best common way to learn and compete on CTF competitions is participates on the Jeopardy-style CTF. Jeopardy-style CTF is like the actual Jeopardy game as the scoreboard looks like a Jeopardy board with different categories and point values. There can be more than two teams as the teams are not trying to attack each other, as seen in Figure 1.

Figure 1 - Jeopardy Style CTF

Some of the challenges can be done against a main server that was developed for the CTF and the flag is inputted into the CTF scoreboard to get points for the team or as individual. A timer is used to start and stop the CTF and once the timer finishes, the game is over. The team or the individual with the most points at the end wins. The focus areas that CTF competitions tend to measure are Exploit Development, Packet Capture Analysis, Web Hacking, Digital Puzzles, Cryptography, Steganography, etc.

As is mentioned before in the paper, this paper focused on a developed webpage, see figure 2, for tutoring people on Capture the Flag competitions (CTF). The webpage is divided on:

- Navigation Bar – this navbar has tabs where the participants can learn news about up-to-date, examples divided by categories, and competitions where they can participate.
- Introduction Section – this is the top section, after the navbar, where the participants will gain knowledge on information about cybersecurity and capture the flag.
- Focus Area Section – this section has four boxes, one per each area, where the participants will gain knowledge on each of the areas.

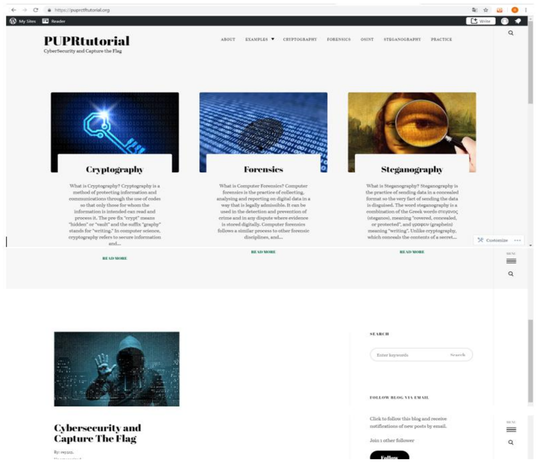

Fig 2 - Homepage of the Developed Webpage

Results and Discussion

Each challenge tutorial exercise example tends to teach a particular set of skills of how to solve a specific problem. As participants complete the tutorials, they gain the knowledge and technical skills to solve the challenge. The following is an overview of the objective before the participants goes into the examples and after they complete the tutorial. They are classified as objectives:

- Objective 1: (Beginnings) Establishes the background information needed to understand each focus area and challenges examples. Which is the Focus Area Section.
- Objective 2: (Cryptography) Allows students to understand how to decode incomprehensible data into meaningful information.
- Objective 3: (Open Source Intelligence) Allows students to investigate to gather intelligence and find the flag for the challenge.
- Objective 4: (Steganography) Allows students to understand how to analyze image or data to uncover hidden information.
- Objective 5: (Web Exploitation) Allows students to understand how to use data from standard infrastructure utilities to obtain information about a target.

Below is an example of how the tutorials are on the webpage:

Challenge Question: A meeting happened at CSU Foothills Campus and one of the agendas was Mock Forecast. We suspect that someone was able to sneak into the meeting by figuring out the meeting id and access code somehow. Can you investigate if the Access code is being leaked somewhere? So, the first thing the participant has to do is open the browser and search for “CSU Foothills Campus Mock Forecast”. Below, Figure 3, shows the search on the browser.

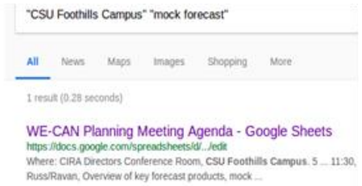

Figure 3 - Browser Search for CSU Foothills Campus

In the browser, we can find a Google Drive document. So, the participant can go ahead an open the document. The Google Drive document shows a spreadsheet like the one that follows on Figure 4.

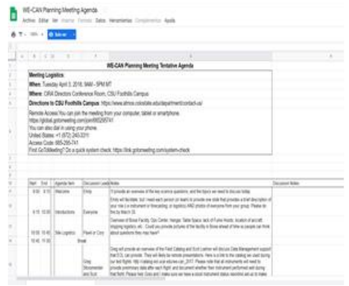

Figure 4 - Google Drive Document of Browser Search

Once we have the google drive document opened, we can just look for the word code or access code or clicking “Ctrl+F” and input the access code. Finally, we have found the code “685-295-741” and just submit the code to get the points.

Conclusions

There has been a steady increase in the number of Capture the Flag (CTF) type of competitions and participation in them by engineering students. Cybersecurity is a relatively young discipline, automatically attracts the attention of internet generation kids and is linked to technology-based competitions like CTF. In the current scenario, there does not exist a frame work to evaluate and rank CTFs. We have created and developed a web page for tutoring people on Capture the Flag competitions (CTF). By completing the tutorials, students are exposed to challenges examples and a tutorial on how to solve and understand each challenge for the skills required for cybersecurity professionals. The developed webpage builds a bridge for students with no cybersecurity knowledge and no access to technological resources to reach an understanding of CTF competitions. We believe that the developed webpage can drastically enhance both quality and quantity of the growing interest in cybersecurity education in K-12, undergraduate (and graduate) university students and workers with no knowledge on this field.

Acknowledgements

This material is based upon work supported by, or in part by the National Science Foundation Scholarship for Service (NSF-SFS) award under contract #1563978.

In addition, I want to thanks my advisor professor, Dr. Jeffrey Duffany, for all his support throughout this project.

References

[1] R. S. Cheung, et al., “Effectiveness of cybersecurity competitions,” in Proceedings of the International Conference on Security and Management (SAM), the World Congress in Computer Science, Computer Engineering and Applied Computing, 2012.

[2] C. Wee and M. Bashir, “Understanding the Personality Characteristics of Cybersecurity Competition Participants to Improve the Effectiveness of Competitions as Recruitment Tools,” Advances in Human Factors in Cybersecurity. Springer Publishing, 2016, pp. 111-121.

[3] R. S. Cheung, J. P. Cohen, H. Z. Lo, and F. Elia, “Challenge based learning in cybersecurity education,” in Proceedings of the International Conference on Security & Management, vol. 1. Las Vegas, Nevada, USA: SAM 2011, Jul. 2011.

[4] C. Eagle and J. L. Clark, “Capture-the-flag: Learning computer security under fire,” Naval Postgraduate School, Monterey CA, 2004.