Cybersecurity Competitive Labs-as-a-Service: Automated Score and Message Board Design

Nicholas Hempenius

Department of Technology Systems
College of Engineering and Technology
East Carolina University
Greenville, NC 27858
hempeniusn15@students.ecu.edu

Te-Shun Chou

Department of Technology Systems
College of Engineering and Technology
East Carolina University
Greenville, NC 27858
chout@ecu.edu

Lee Toderick

Department of Technology Systems
College of Engineering and Technology
East Carolina University
Greenville, NC 27858
toderickl@ecu.edu

ABSTRACT

There has been extensive research and analysis of the effectiveness of game-based education tools, however there is limited literature on the designs of such tools. The Automation of collecting scoring metrics within virtualized cyber-attack and defense games can be a complicated task. It required robust, accurate, and fast technology. A means of keeping the integrity of the score must also be in place. In this presentation we presented a novel design of an Automated Scoring and Message Board (ASMB) system, which was developed under a five-step methodology and used in a Competitive Labs-as-a-Service (CLaaS) platform.

Keywords

Cybersecurity; cybersecurity games; Competitive Labs-as-a-Service

1. INTRODUCTION

Addressing the talent gap, and lack of Cyber security professionals, there has been a leap towards research in how to educate the future cybersecurity work force. A class of Serious Cybersecurity Games is cybersecurity CLaaS. CLaaS is an all-in-one package that can be deployed at an extremely low cost as a supplementary cybersecurity education tool. This concept is young in name, but similarly designed platforms are nothing new [1][2]. The CLaaS referred to, in this presentation, presented a restricted access VM-based environment for students [1]. Although there has been much literature created on best practices and designs of cybersecurity wargames, exercises, and game-based educational tools, few present technical specifications of the designs [2]. This presentation addressed the design of an ASMB system in technical terms, specific to a new approach using VM-based environments, CLaaS.

2. METHODOLOGY

The methodology behind achieving these goals was independent of score values and the measurement points of learning objectives. The methodology contained five steps that were addressed sequentially as follows; Continuous Collection of

Objective based data points; Secure transportation of collected data; Secure storage of collected data; and Analyze data to create scoring metrics; and A comprehensive display of scores to participants.

3. CONCLUSION

The purpose of the ASMB was to produce comprehensive output and display it in a user-friendly manner. Step 1 was to have a continuous collection of data. The purpose of this step was to create a flow of data to be analyzed. Using a heartbeat Terminate and Stay Resident (TSR) script, it was possible to log relevant data continuously. Using tools, such as WinRAP in Windows, or configuring the "hidepid" option in Linux, we can hide the heartbeat scripts from even privileged users. Step 2 addressed a common tradeoff in cybersecurity between speed and security. We determined the transportation of the collected data was to be placed onto a dedicated ASMB network. Also, utilizing a hidden TSR heartbeat logging script that transmits logs as a Rsyslog agent with TLS. Step 3 addressed storing the data. The data stored needs to be a common format, and in a secure location. A firewall placed between the environment VMs and the Rsyslog server on the ASMB network was likely all that was needed to provide stored data integrity. In Step 4 we analyzed the data. Derived output from the data needed to produce a score and a message directed at the student. Step 5 was the final step where the output of the data was presented to the score and message board. This step allowed for the most creativity. A simple table could have been created and displayed on a web interface using a simple PHP script that requires a database.

4. ACKNOWLEDGMENTS

This research is made possible by the National Science Foundation under grant 1723650. The authors are grateful to the support of the Department of Technology Systems in the College of Engineering and Technology at East Carolina University.

5. REFERENCES

- [1] Brilingaitė, A., Bukauskas, Li., Kutka, E. 2017. Development of an Educational Platform for Cyber Defense Training. In *Academic Conferences International Limited*. (Jun 2017), 73-81.
- [2] Masas, S., Hallaq, B., and Maennel, O. 2017. Obtaining Better Metrics for Complex Serious Games Within Virtualised Simulation Environments. In *European Conference on Games Based Learning*. Academic Conferences International Limited, United Kingdom, Reading, 428-434.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.

SIGITE '18, October 3-6, 2018, Fort Lauderdale, FL, USA

© 2018 Copyright is held by the owner/author(s).

ACM ISBN 978-1-4503-5954-2/18/10.

<https://doi.org/10.1145/3241815.3241825>