2021 ASEE ANNUAL CONFERENCE
Virtual Meeting | July 26–29, 2021 | Pacific Daylight Time
Paper ID #32282

Lab Performance Evaluation via a Workshop Survey

Dr. Te-Shun Chou, East Carolina University

Dr. Te-Shun Chou is a Professor in the Department of Technology Systems (TSYS) at East Carolina University (ECU). He received his Bachelor degree in Electronics Engineering at Feng Chia University and both Master's degree and Doctoral degree in Electrical Engineering at Florida International University. He serves as the program coordinator of the Master program in Network Technology for TSYS and the lead faculty of Digital Communication Systems concentration for the Consortium Universities of the Ph.D. in Technology Management. He is also the point of contact of ECU National Centers of Academic Excellence in Cyber Defense Education (CAE-CDE). Dr. Chou teaches IT related courses, which include cyber security, intrusion detection and incident response, wireless communications, and network management. His research interests include machine learning, wireless communications, technology education, and cyber security, especially in the field of intrusion detection systems.

Dr. Biwu Yang, East Carolina University

Dr. Biwu Yang is a professor in the Department of Technology Systems, College of Engineering and Technology, East Carolina University. He teaches in the field of data networking, information technology, and information security. He has served as the key technology person in all aspects of Global Academic Initiatives since its inception, with multiple projects that include more than 30 partner universities from more than 20 countries, and the Global Climate Change course including Brazil, China, India, Mexico and USA.

Lab Performance Evaluation via a Workshop Survey

Abstract

We implemented a unique learning system, Competitive Labs-as-a-Service (CLaaS), that provided comprehensive cybersecurity awareness education. The system included multiple identical virtual learning environments. Each learner had his/her own learning environment and multiple virtual machines (VMs) were nested in each environment to serve both tasks of attack and defense. A graphic user interface (GUI) application was designed to provide access to the environment where cybersecurity activities were performed. The application menu included a set of CyberSec labs, each containing a pair of attack and defense sub-labs. Each sub-lab is a combination of both cybersecurity theory and practice.

A workshop was held in the summer 2019 in the Department of Technology Systems (TSYS) at East Carolina University (ECU) in the summer of 2019. Nineteen college instructors were invited to use the system and participated in a survey in the end of the workshop. In this paper, we discussed the survey results of both the learning environment and the CyberSec labs.

Keywords: Cybersecurity; virtualization technology; cyberattack; cyber defense

1. Introduction

With the evolution of technology, the internet has become an indispensable aspect of our daily life. In the meantime, cybersecurity threats seek to breach the information system of both individuals and organizations. According to the Cyber Incident & Breach Trends Report released by The Internet Society's Online Trust Alliance (OTA), there were more than 2 million cyber incidents in 2018 which caused an overall financial impact of at least $45 billion worldwide [1]. In the U.S. alone, the Internet Crime Complaint Center (IC3) received more than 20,000 incident complaints with losses of over $1.2 billion [2]. Hence, the U.S. government has placed cybersecurity as a national priority in order to minimize damage from cyber incidents. In the fiscal year of 2019, the President's Budget included $15 billion of budget authority for cybersecurity-related activities to improve the security and resilience capabilities of national information infrastructures [3].

In addition to the efforts made from the government in national cybersecurity protection, it is also important that everyone should receive a basic training of cybersecurity concepts and techniques. The National Initiative For Cybersecurity Careers and Studies (NICCS) stated: "We must teach science, technology, engineering and math (STEM), and other cyber concepts to all students, and educate all students on the secure use of today's ever-evolving technologies." [4].

In order to meet our country's need, a learning system, CLaaS, was developed to foster highly educated and skilled cybersecurity professionals to protect our nation's critical cyber infrastructure. The system included a set of CyberSec labs and was designed to be adapted for multiple uses. Leveraging virtualization technology and a user-friendly GUI application, learners can access the system anytime and anywhere in the world to practice cyber-attack and cyber-defense techniques. Upon completion of the cybersecurity activities included in the system, learners will be well-prepared and ready to contribute their knowledge and hands-on experiences in cybersecurity to a high demand workforce.

In order to promote the system visibility to other colleges, a two-day workshop was held in the

summer 2019. Nineteen college instructors attended the workshop and participated in a survey at the end of the workshop. The survey included a set of questions related to the workshop and the learning system. In this paper, we focused on the discussion of the labs and the learning environment. We hope the evaluation could identify whether the degree of difficulty of designed labs is appropriate or not. The project team can then revise the lab contents to improve the overall quality of the system.

This paper is organized as follows: Section 2 introduces the CyberSec labs. Section 3 describes the questionnaire. Section 4 the survey results. Finally, we conclude our work in the last section.

2. CyberSec Labs

In the learning system, a GUI application was designed to help learners navigate the system [5]. In total, eight CyberSec labs were designed: Web defacement lab, Remote secure login lab, FTP server DoS lab, Patch management lab, Backdoor lab, SQL injection (SQLi) lab, Honeypot lab, and Secure plain text traffic labs. Each lab included two sub-labs (attack and defense) and objectives were included in each of the labs. Figure 1a displays the GUI application and Figure 1b shows the two sub-lab buttons after clicking the Secure remote login lab. Table 1 shows the CyberSec labs and their corresponding objectives.

(a) (b)

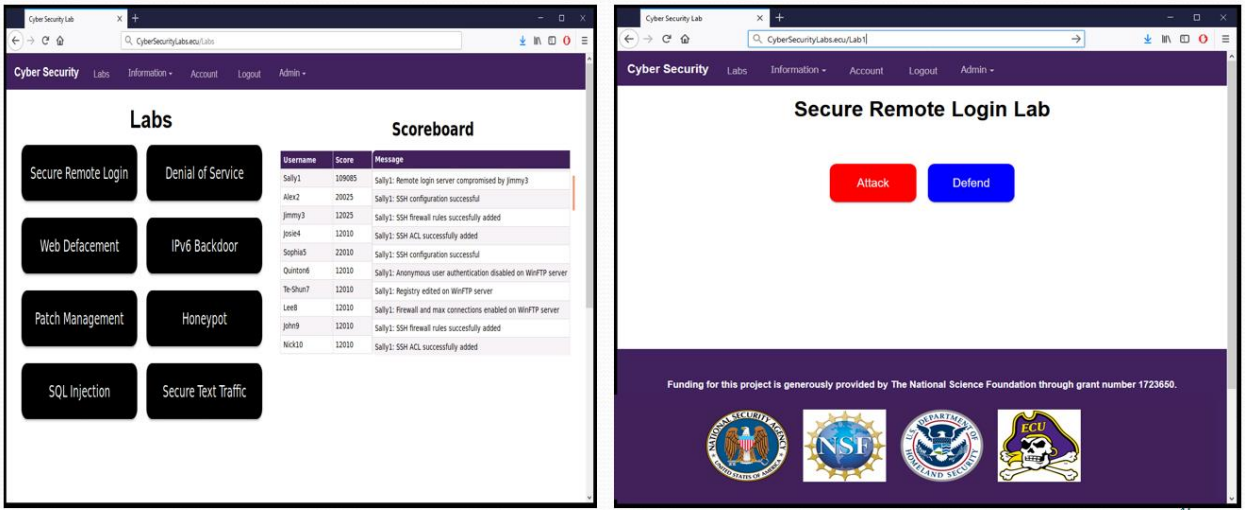

Figure 1. (a) CLaaS GUI application (b) Sub-labs of secure remote login lab

Table 1. CyberSec Labs and Objectives

Lab	Attack sub-lab objectives	Defense sub-lab objectives
Secure Remote Login	• Use security scanner to enumerate target host and identify the listening Secure Socket Shell (SSH) service port on target host • Use password profiler to generate a wordlist of candidate passwords	• Edit the openSSH configuration file to restrict root user from logging in via SSH • Add rules to the host iptables firewall, limit the amount of connections to the SSH service over a period of time, and temporarily block connections from any host that goes over the defined limit

	• Perform brute force attack to discover the root password on a target host and then login to change the password	• Create an Access Control List (ACL) for SSH using host firewall iptables
FTP Server DoS Attack	• Scan the target network for possible vulnerabilities in the open ports • Access the FTP server through an anonymous user account • Bring down the FTP server after sending SYN flood packets	• Configure Windows Server to turn on the firewall and change the default value on maximum connections to the FTP data • Deactivate the anonymous user authentication to prevent unwanted access into the network • Edit the Windows Server's registry to activate the SYN protect key against the SYN flooding attack
Web Defacement	• Create a new user's account on a web page and inject malicious codes into the comment box • Deface the webpage	• Set up the firewall iptables to filter unwanted packets from the network • Sanitize the strings by filtering the input on the PHP login page • Run malicious codes on the sanitized webpage to identify possible vulnerabilities
SQL Injection	• Scan the network for possible vulnerabilities on the open ports • Run a login bypass on the victim's web address • Use SQL injection and database takeover tool to discover vulnerabilities and steal information from the database, e.g., passwords • Use a syntax to replace the old password stolen from the database with a new password	• Set up firewall iptables to filter unwanted packets from the network • Sanitize the strings by filtering the input on the PHP login page • Run a login bypass and check for potential weaknesses
Patch Management	• Use network mapper to discover running network services • Use open vulnerability assessment system to scan for network vulnerabilities on a target computer • Exploit a vulnerable service on the target computer to gain access and modify files	• Use network mapper to discover running network services • Use open vulnerability assessment system to scan for network vulnerabilities on the target computer • Patch outdated and vulnerable services
Backdoor	• Discover all live hosts on the network • Use penetration testing tools to run a port scan and exploit the IPv6 auxiliary modules • Create a persistent backdoor on a target host • Retrieve files from the victim	• Close unnecessary ports • Set up firewall to block traffic on SMB over IP port
Honeypot	• Change the honeypot architecture information • Customize honeypot files • Create replica files in the honeypot file system	• Install the prerequisite packages needed for the honeypot • Install required python packages • Move the listening port before creating the honeyport • Configure the honeypot
Secure Plain Text Traffic	• Determine if an FTP server allows anonymous access or if it is password-protected	• Determine that an FTP server is unsecured

	• Use tcpdump to sniff network packets • Examine network packets using Wireshark • Access FTP server with discovered credentials and download target file	• Generate SSL keys for secure communication • Configure VSFTPd for secure FTP access and transmission • Verify that an FTP server is secure

In order to help learners acquire both theoretical cybersecurity knowledge and practice hands-on cyber-attack or cyber-defense activity, a three-stage learning process was employed in each sub-lab [6]. In Step 1, a certain type of attack/defense was introduced. In Step 2, learners must demonstrate that they have mastered the relevant knowledge shown in Step 1. Ten random questions were displayed at a time and each question was worth 10-points. Learners needed to score a minimum of 80-points on the quiz in order to move on to the next step. In Step 3, a detailed attack/defense instruction was shown to guide learners step-by-step to launch an attack or implement a defense mechanism. In addition, the system functioned as a competitive environment that encouraged learners to interact with each other. Learners who successfully completed an objective gained one thousand points; conversely, learners who did not implement a defense mechanism to prevent the corresponding attack lost one thousand points. This game-based learning strategy not only stimulated interest in learning the subject matter but also made learning more exciting. Figure 1a shows the Score and Message Board [7, 8] that displays the instant messages and the scores of learners.

3. Questionnaire

An exit survey was conducted during the second day of the workshop. Google Forms was used for designing the survey [9]. The survey questions included four major parts: (1) Questions related to self-assessment of knowledge level in the subjects of cybersecurity (before and after attending the workshop), (2) Questions related to the workshop, (3) Questions related to the learning environment, and (4) Questions related to the labs. The type of questions were five-level Likert scale questions and short answers. Some questions' responses were "5 = Excellent. 4 = Very Good. 3 = Good. 2 = Fair. 1 = Poor" and some were "5 = Strongly Agree, 4 = Agree, 3 = Neutral, 2 = Disagree, and 1 = Strongly Disagree".

In this paper, we focused on the discussion of the survey results of lab related questions. Based on the survey outcomes, the development team could then make proper adjustments to improve the usefulness and effectiveness of the system. In addition, the survey results would be helpful to improve the appropriateness of the system's contents to better accommodate student learning. Tables 2 and 3 show the survey questions of labs and lab environment, respectively.

Table 2. Lab survey questions

Number	Question
Q.L.1	The labs were relevant to current cybersecurity technology and methods.
Q.L.2	The introductions were helpful in understanding the theoretical knowledge of cybersecurity topics.
Q.L.3	The quizzes were helpful reinforcing information learned from the introduction.
Q.L.4	The lab walkthroughs were helpful in getting practical experiences of cybersecurity.
Q.L.5	The lab walkthroughs were clear enough in completing hands-on tasks.

Q.L.6	The three-stage learning (introduction, quiz, and lab walkthrough) is a good idea for teaching cybersecurity.
Q.L.7	I encountered no difficulties when doing the labs.
Q.L.8	The score and Message Board made learning interesting in an interactive environment.

Table 3. Lab environment survey questions

Number	Question
Q.LE.1	The performance of the lab environment was satisfactory.
Q.LE.2	The performance of the virtual machines in the labs was satisfactory.
Q.LE.3	The graphic user interface (GUI) was intuitive and easy to use.
Q.LE.4	Graphics, fonts and images were legible and easy to read and understand.
Q.LE.5	The simulated lab environment felt realistic, like using real world servers.
Q.LE.6	I had no difficulties logging on the lab environment to conduct required activities.
Q.LE.7	It's a good strategy to imitate complicated networks by using virtualization technology.
Q.LE.8	I expect to use this lab environment at my organization to teach cybersecurity courses.
Q.LE.9	I would recommend using this lab environment to other faculty.
Q.LE.10	The lab environment is user-friendly and felt reliable, secure, and easy to access and operate.
Q.LE.11	The lab environment enables the learner to complete a sequence of cybersecurity activities at his or her own pace, anytime, and from anywhere. This self-guided approach makes learning enjoyable and is effective in improving student learning and understanding.

4. **Survey Results**

There were nineteen College instructors attending the workshop and all of them participated the exit survey. Figures 2 and 3 display the survey results of lab questions and lab environment questions, respectively.

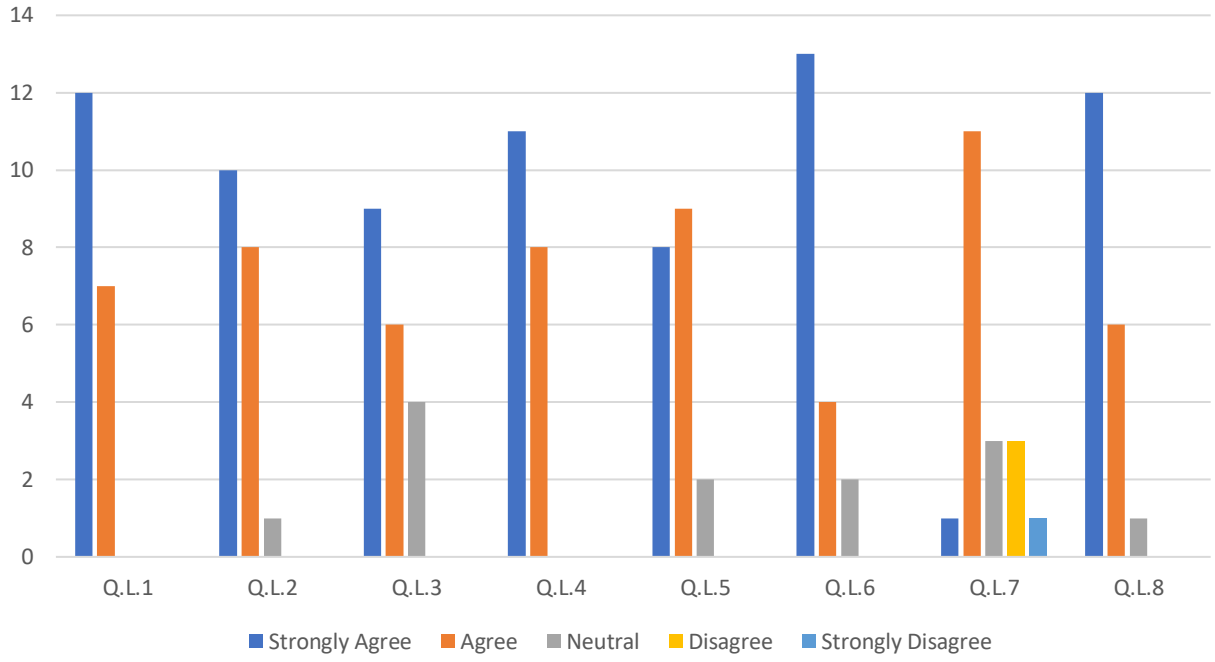

Figure 2. Survey result of lab questions

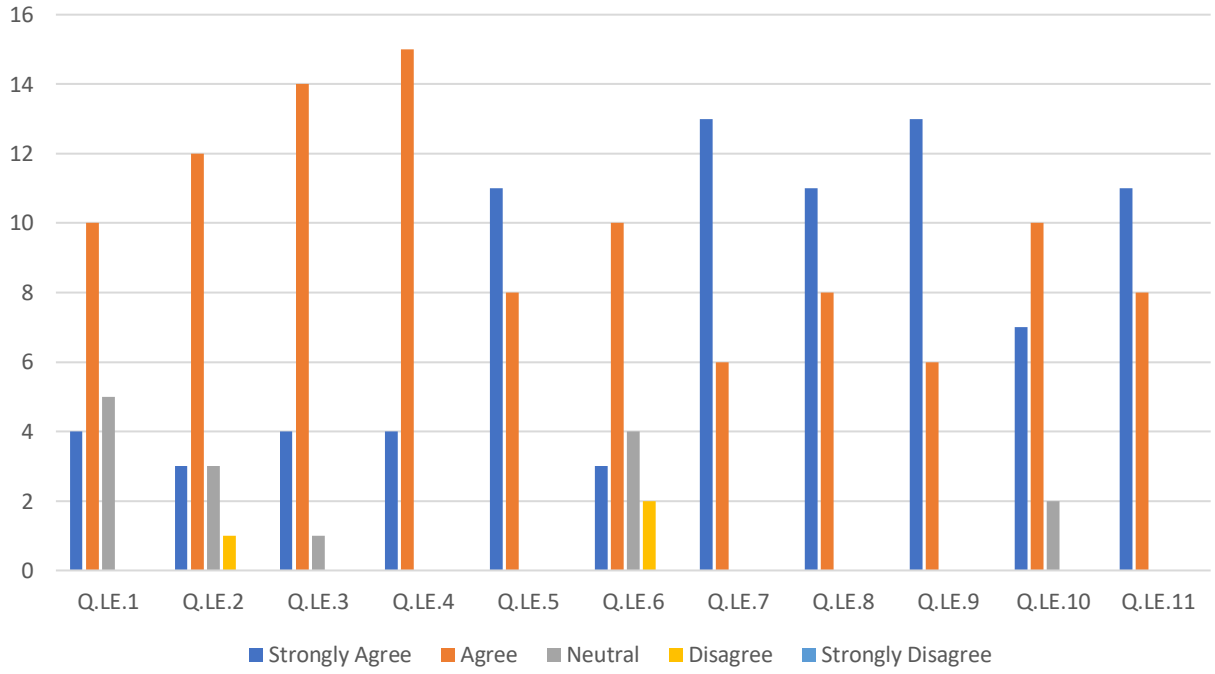

Figure 3. Survey result of lab environment questions

For Q.L.1, Q.L.4, Q.LE.5, Q.LE.8, Q.LE.9, and Q.LE.11, all of the responses fell into the categories of Strongly Agree and Agree. For Q.L.3, four respondents proclaimed themselves Neutral about the question. The same finding was also observed in the question of "What do you dislike most about the lab activity?". Eight respondents revealed that taking the quizzes was their

least favorite lab activity. This was due to the fact that perhaps some of the learners were eager to conduct the hands-on lab activity and hence did not pay too much attention in the reading of the introductions thoroughly, which resulted in them having to take a quiz multiple times in order to move on to the last step. As for the question of "What do you like most about the lab activity?", all of the respondents indicated that conducting the hands-on lab activities was their favorite part. Only five respondents expressed that they enjoyed the reading of introductions and four respondents desired to take the quizzes.

For Q.L.7, almost half of the respondents encountered technical matters while using the learning system. The issues included login problem, VMs were slow to respond, and sometimes the screen froze that needed to be refreshed. Similar responses can also be found in the results of questions of Q.LE.2 and Q.LE.6. These problems need to be further investigated and could probably be resolved by adjusting memory-related settings on VMs as well as by adding more memory to promote both VMs and overall system performance.

In general, the survey results showed that the respondents had a positive attitude toward all of the lab and lab environment questions. In addition, the multiple-choice question "What educational level do you feel these labs should be presented?" was asked. As shown in Figure 4, 64% responses thought the labs were suitable for sophomore or junior level students to get training of cybersecurity awareness.

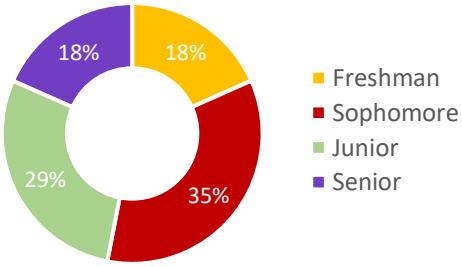

Figure 4. Appropriate education level for conducting the lab activities

Conclusions

The learning system, CLaaS, was offered in a train-the-trainer format in the summer 2019. The workshop introduced the system and provided nineteen college instructors with opportunities to gain theoretical concepts and exercise practical skills. The objective of the workshop was to help college instructors learn the system so they could go back to their own institutions and enhance the overall quality of cybersecurity education. At the end of the workshop, a survey was distributed to evaluate the system performance. In general, the survey results showed that the workshop attendees were satisfied with the CyberSec labs and the lab environment. All of them agreed that the labs were relevant to current cybersecurity technology and the lab environment was realistic, like using real world servers. Even though some of the attendees encountered technical issues during the workshop, all of them were still willing to recommend the system to their colleagues and looked forward to using the system at their own organizations to teach cybersecurity courses.

Acknowledgements

This research is based upon work supported by the Secure &Trustworthy Cyberspace (SaTC) Program of the National Science Foundation under Grant Number 1723650. The authors are grateful to the support of TSYS in the College of Engineering and Technology at ECU. Thanks also go to our Information Computer Technology (ICT) Advisory Board and Mr. Kelly Caudle for their efforts to broadcast the workshop recruitment information and those who attended the workshop.

References

1. K. Olmstead, 2018 Cyber Incidents & Breach Trends Report, Internet Society's Online Trust Alliance (OTA), Kenneth Olmstead. Retrieved from: https://www.internetsociety.org/blog/2019/07/internet-societys-online-trust-alliance-2019-cyber-incidents-breach-trends-report/
2. M. Gorham, 2018 Internet Crime Report, Internet Crime Complaint Center. Retrieved from: https://pdf.ic3.gov/2018_IC3Report.pdf
3. Cybersecurity Funding, The White House. Retrieved from: https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf
4. Formal Education, The National Initiative For Cybersecurity Careers and Studies (NICCS). Retrieved from: https://niccs.us-cert.gov/formal-education#
5. W. Hotalen and T. S. Chou, "A Multiplayer Peer-to-Peer Cyber Attack and Defense Infrastructure," *American Society for Engineering Education (ASEE) Annual Conference and Exposition*, Salt Lake City, Utah, June 2018.
6. T. S. Chou, "Labs and Three-Stage Learning Process for a Cyber Security Learning System," *International Conference on Engineering, Science and Technology (IConEST)*, Denver, CO, October 2019.
7. N. Hempenius, Te-Shun Chou, and Lee Toderick, "Automatic Collection of Scoring Metrics in Competitive Cybersecurity Lab Environments," *The Conference for Industry Education Collaboration (CIEC)*, New Orleans, LA, January 2019.
8. N. Hempenius, T. S. Chou, and L. Toderick, "Cybersecurity Competitive Labs-as-a-Service: Automated Score and Message Board Design," Lighting Talk, *The Annual Conference on Information Technology Education (SIGITE)*, Fort Lauderdale, FL, October 2018.
9. Google Forms. Retrieved from: https://www.google.com/forms/about/