Proceedings of IEEE International Conference on Applied System Innovation 2018
IEEE ICASI 2018- Meen, Prior & Lam (Eds)

Design and Implement of Capture the Flag based on Cloud Offense and Defense Platform

Kai Chain[1*], Cheng-Chung Kuo[2], I-Hsien Liu[2], Jung-Shian Li[2] and Chu-Sing Yang[2]

[1]Department of Mechanical Engineering Department of Computer and Information Science,
R.O.C. Military Academy, Kaohsiung 830, Taiwan.
*chainkai@mail2000.com.tw
[2]Institute of Computer and Communication Engineering, Department of Electrical Engineering,
National Cheng Kung University, Tainan 701, Taiwan.
jjguo@crypto.ee.ncku.edu.tw, ihliu@twisc.ncku.edu.tw, jsli@mail.ncku.edu.tw, csyang@mail.ee.ncku.edu.tw

Abstract

The future war pattern will launch attack immediately and carry on face-to-face combat. Consequently, every type of network attacks, defense, and competitions will be paid attention by all countries. The research will make use of Testbed at ROCMA and Cyber Defense Exercise platform to begin the network attack-and-defense drill of Capture The Flag. Regard the practice and the exchanges as principle, the participants will acquaint with invading and defense method.

Key words: Information security, network testbed, Cyber Defense eXercise, Capture the Flag

Introduction

Following an increase in cyberattacks, a growing number of countries and government institutes have invested resources in reinforcing cybersecurity education. Exceptional students from governments, enterprises, and schools in South Korea participated in the Best of Best cybersecurity human resource training program in 2010, and won the DEFCON Capture-the-Flag (CTF) [1] cybersecurity competition in 2015. The United States government announced a Cybersecurity National Action Plan to strengthen its cybersecurity as well as that of its private sector [2]. Parts of the budget for the plan involved training cybersecurity talent because of the shortage and high demand for cybersecurity experts that the country faces. These talent training programs, including military programs for cybersecurity force reserves, provide cybersecurity scholarships, which require that students work in government sectors to acquire them. Furthermore, these programs feature uniform cybersecurity education courses to provide graduating students with sufficient skills for government cybersecurity jobs. Additionally, employees who intend to work in federal cybersecurity units are exempt from loans. These incentives may inspire extraordinary cybersecurity talent and hackers to work in government sectors.

An increasing number of cybersecurity competitions such as CTF, attack and defense, and penetration tests have been organized. Today, the US military continues to organize an interdepartmental network series of exercises named Cyber Storm, which involve using real network connections to simulate cyberattacks against critical infrastructures, thereby enabling the military to understand and assess the capability of each agency to meet and respond to real cyberattacks. The US military acknowledges that the capability of hackers to attack is comparable to—and presumably more dangerous than—that of a national armed force. The North Atlantic Treaty Organization annually organizes transnational cybersecurity exercises named Locked Shields [3] to evaluate the capability and time of each country to respond to related cyberattacks.

Real network defense and penetration test competitions, which require constructing experimental environments and training participants in advance, involve more complex personnel, software, and hardware preparations than those of general CTF competitions. Therefore, the cybersecurity competitions at present are primarily organized as CTF competitions.

In a CTF competition, the organizers design relevant questions to test the participants, who log into the answering system and answer the questions. Scores are awarded on the basis of the difficulty level of each question, the number of participants that succeed in solving the question, and the amount of time taken to solve it. After the test is concluded, the participants are ranked according to their scores.

This study examined the structure of a CTF competition organized through the use of the cyber defense exercise (CDX) platform provided by the National Center for High-Performance Computing (NCHC) [4]. Students across Taiwan were invited to the competition to assess the applicability of its structure, and the evaluations by the participants after the competition were gathered to improve the system.

The remainder of this paper is structured as follows. Section 2 reviews relevant studies; Section 3 presents the CDX structure applied in this study; Section 4 reports the CTF competition organized through the use of the structure; and Section 5 concludes the paper and addresses suggestions for future studies.

Related work

A. Capture-the-Flag

CTF is a distinguished form of cybersecurity competition similar to a war game. A number of questions are presented during the competition, and participants receive points corresponding to the questions they answer correctly. The types of question include Web, digital identification, disassembly, and packets. Scores are rewarded according to the difficulty

ISBN 978-1-5386-4342-6

level of the questions solved.

Currently, the most famous hacking competition worldwide is DEFCON, which is engaged in by contestants from around the world and hosted annually in Las Vegas, United States. First, participating teams must pass the qualification rounds (DEFCON CTF Qual), which are organized as CTF rounds. Subsequently, the final 10 qualifying teams partake in attack and defense rounds. Generally, information regarding an open CTF competition can be acquired through the CTF Time website [7]. The forms of CTF competitions presented on the website include Jeopardy and attack and defense.

A relevant study [5] indicated that a typical CTF competition requires basic technical security knowledge and months of dedicated preparations to participate in. Thus, the challenge of entering the competition is particularly high. The study maintained that competitions should focus on raising enthusiasm in students. Another study [6] demonstrated a platform based on an offline virtual machine, on which students were only required to download a completed virtual machine to participate in the CTF competition. The learning outcomes of the students regarding specific fields were assessed according to the correct answers submitted by the students pertaining to those fields. A third study [8] alluded to an education cycle, which involved confirming a course (contents to teach and learn), teaching (methods to teach and learn), and evaluating (approaches to assess the learning results). Overall, CTF is an ideal evaluation approach in cybersecurity education.

B. Cyber Defense Exercise

Recent major cybersecurity incidents, which have incurred sensitive information leaks and financial losses in affected units, have led to increased government attention to cybersecurity. Using their years of experience in practicing cybersecurity and developing platforms, the NCHC established the first CDX platform in Taiwan. Through the use of the rapid deployment and flexible resource allocation capabilities of the Cloud structure, the problems in creating cybersecurity course environments involving conventional structures were solved, and an ideal environment was formed for cultivating practical cybersecurity talent.

The core structure of the CDX platform is based on Ezilla core technology by the NCHC and the concept of "Carry on Cloud," which eliminates the need for reformulating systems for specific users. The platform automatically generates images of customized virtual nodes according to the users' requirements, which profoundly lowers the limitations they face in using cloud resources, facilitates independent operating spaces for users, and enables rapid and easy access to applications from the cloud.

The original application scenarios were divided into research, penetration tests, malware analysis, and cybersecurity tool examination. However, because of an increase in the popularity of CTF competitions, CDX platforms were also used to generate scenarios that users and teachers could choose. When users complete their account registration, they can connect to the system through a virtual private network (VPN). All operations are completed on CDX platforms, and users do not interfere with one another because their experimental environments are incompatible with one another.

System Architecture

The competition demonstrated in this study was divided into preliminary and intermediary rounds, which featured systems distinct from each other. The systems and evaluation methods adopted in the preliminary and intermediary rounds are described as follows:

A. Preliminary round

The preliminary round concerned the participants' knowledge and understanding regarding cybersecurity, and comprised online tests. These tests featured multiple choice questions that featured both single and multiple answers. Thus, the main purpose of the preliminary round was to assess the academic competencies of the participants. Since the CTF need basic technical security knowledge and trainings, the preliminary round can filter participants.

B. Intermediary round

The participants that passed the preliminary round qualified for the intermediary round, the purpose of which was to evaluate their practical competencies. The users logged into the systems and read and answered the questions. The system of the intermediary rounds comprised an environmental module, scoring module, and follow-up review, as shown in Fig. 1.

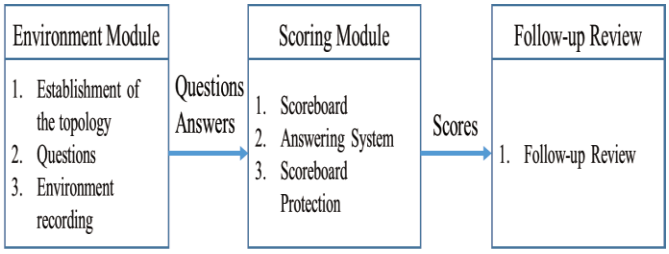

Fig. 1. System structure of the intermediary round.

1. Environmental module

This module was intended to create the execution environment required for the exercise. Established environments, related operation systems, engine vulnerability, test questions, and environment generation records enabled accomplishing experiment establishment processes in decreased amounts of time in subsequent retests.

The primary functions of this module are as follows: (a) Selecting scenarios: The users can select their desired scenarios for the test, such as Web infiltration tests, engine vulnerability scanning, distributed denial-of-service attacks, and simple CTF scenarios. (b) Establishing the topology: After the users chose their topologies, the system distributed default network topologies to them; the users could add related attack and defense nodes into their topologies as desired during this phase. (c) Test questions: The test questions primarily involved problem-solving; related questions were implemented in the system for the users to solve during the establishment of the experiment. (d) Recording information: After the test was concluded, the related nodes, software, and topologies were recorded into the system to allow the users to rapidly create their environments when repeating the tests.

ISBN 978-1-5386-4342-6

2. Scoring module

This module was designed for monitoring the scores and test progress of the participants. The participants read the current progress of their teams on the webpages and learned about the remaining questions to be solved. The main functions of this module are described as follows: (a) Scoreboard: The Web-based interface displayed the current scores and test progress of the participants and their respective units. (b) Answer system: After acquiring the keys for the questions or completing the required objectives, the users entered the keys in the answer system to verify that they had solved the questions and earn relevant scores. (c) Scoreboard protection system: The scoreboard, which recorded the scores and progress, was one of the most vulnerable spots in the system for attacks by participants. Because the participants might crack or attack the keys using brute force methods, a protection mechanism was required for the system. For example, a 60-s interval was enforced between each key upload.

3. Follow-up review

This module was established for the participants to express feedback regarding the test after its conclusion. The scores were one of the objects of review. Additionally, if the number of participant units increased, then the participant units or students could be compared with one another for the methods they implemented.

Evaluation

A competition was held in May 2017 to verify the applicability of the system, and students across Taiwan were invited. A total of 79 teams (132 participants) partook in the competition, and 32 teams (59 participants) qualified for the intermediary round.

The competition process comprised preparations, test processes, and follow-up reviews. The preparations involved establishing the experiment environment, uploading the questions, and training the participants in engaging in the competition.

The preliminary round, which comprised online tests, involved the participant teams answering the questions in the answer system through network connections (Fig. 2).

The average rate of correct answers in this round was 34%. Of the highest number of questions answered by a team (125), only 20.1% were answered correctly, indicating that the team answered by guessing; therefore, the team was disqualified.

A question appeared when the participant clicked on one of the green boxes; any successfully solved key had to also be entered in this interface. To prevent users from cracking the keys, the interval between each answer input was set as 30 s; hence, the user had to wait for 30 s to answer again after submitting an incorrect answer (Fig. 3).

The scores in the intermediary round were dispersed. For a total of five participants, the two joint first place participants answered a total of 14 questions correctly; second place participants answered 8 questions correctly; third place answered 7 correctly; and fourth place answered 6 correctly. This competition, originally intended for college and university students, presented no age limit for participants and included high school students among its participants. This indicated that cybersecurity education had been extended to students of lower ages.

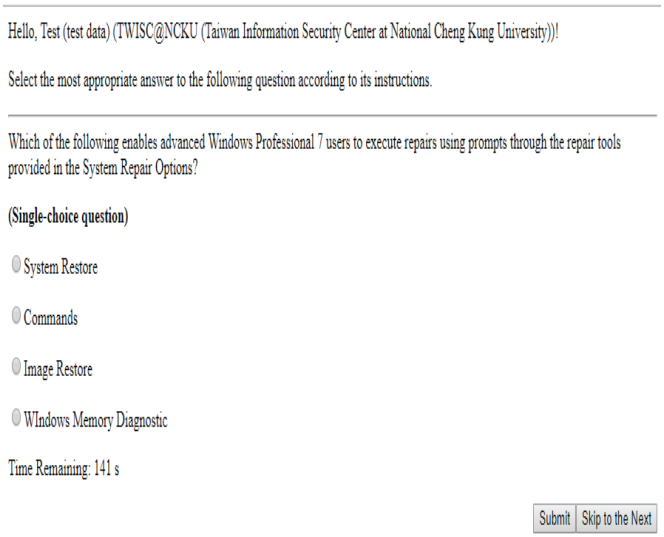

Fig. 2. Answer system in the preliminary round.

Student responses

Feedback questionnaires were distributed after the end of the competition. The responses by the students and staff members were organized as follows:

Time of the tests:

All of the test questions in the intermediary round were practical questions. Students who were unfamiliar with the related operations and problem-solving skills might have expended excess time solving the questions.

Difficulty levels of the questions:

Because all participants joined the competition of their own volition, those that passed the preliminary rounds varied considerably in the level of their skills relevant to the competition; moreover, they perceived the difficulty levels of the same questions differently. According to the participants' interviews, the system of the CTF competition was oriented toward practical implementations, and its demand for the problem-solving proficiency of participants was high. Therefore, the scores of the participants of higher ranks were substantially superior to those of the participants of lower ranks in the intermediary round.

System proficiency:

Several participants responded that the CDX platform was particularly challenging to master, and the activities could easily be limited to the platform. Although attack and defense tests were excluded to prevent this situation, as well as only CTF questions being adopted in this competition, logging into the VPN system on the CDX platform remained mandatory.

ISBN 978-1-5386-4342-6

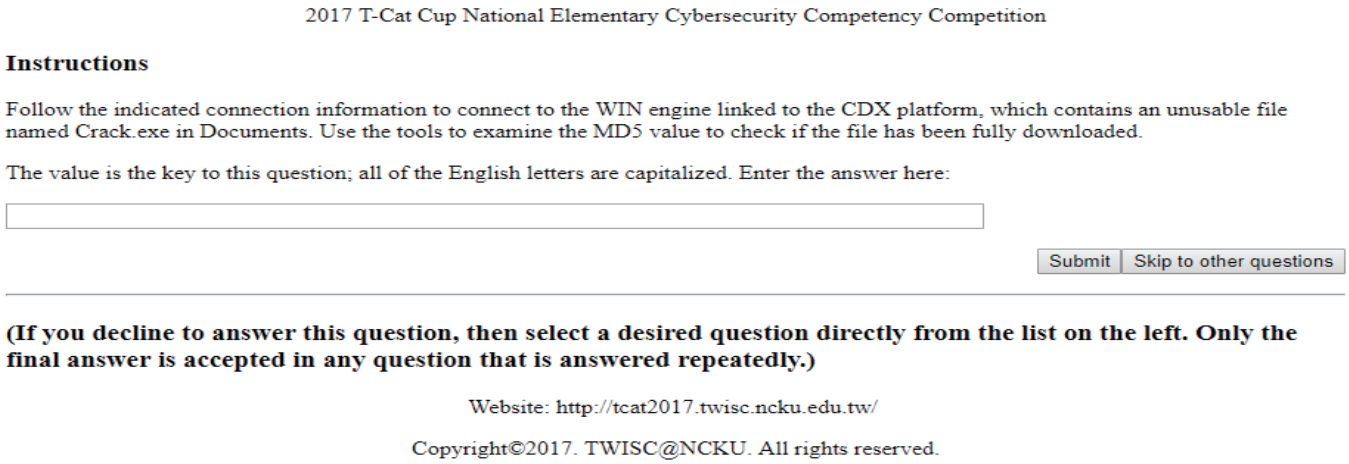

Fig. 3. Answer system.

Conclusion

According to this study, designing, planning, and implementing the CTF competition enabled the participants to acquire knowledge pertinent to cybersecurity and its defense mechanisms and inherit related experience. Moreover, the participants could reconsider their information operation approaches in an ordinary or limited environment. Furthermore, the competition led to the discovery of the directions and problems regarding future CDX platform improvement, such as the types of CTF question required and the accumulation and maintenance of image files. These factors require not only gathering and analyzing data, but also associating the data with various question difficulty levels and estimating the time required to complete questions. For example, predicting the time of successful attacks through the use of various tools involves recording the characteristics of problem-solving processes as packets or saving the records in databases, thereby increasing the flexibility of the tools' future use.

In addition to CTF competitions, CDX platforms can be utilized to design attack and defense or penetration scenarios according to user requirements. Therefore, in conjunction with gathering and analyzing CTF questions, creating various attack and defense exercise scenarios and constructing penetration processes are critical for further research and implementation. Strengthening CDX defense services is essential in human resource training for cybersecurity and network defense technology.

Acknowledgment

The authors would like to thank the Ministry of Science and Technology of Taiwan, for financially supporting this research under Contract Nos. MOST 106-3114-E-001-001 - , MOST 106-3114-E-006-003 - and MOST 106-2221-E-145-002-.

References

[1] COWAN, Crispin, et al. Defcon capture the flag: Defending vulnerable code from intense attack. In: DARPA Information Survivability Conference and Exposition, 2003. Proceedings. IEEE, 2003. pp. 120-129.

[2] Luiijf, Eric, Kim Besseling, and Patrick De Graaf. "Nineteen national cyber security strategies." International Journal of Critical Infrastructures 6 9.1-2 (2013): pp.3-31.

[3] NATO, CCDCOE. "Locked Shields 2016 After Action Report." *NATO Cooperative Cyber Defence Centre of Excellence Publication* (2016).

[4] National Center for High-performance Computing. https://www.nchc.org.tw/

[5] Vitaly Ford, Ambareen Siraj, Ada Haynes, and Eric Brown. 2017. Capture the Flag Unplugged: an Offline Cyber Competition. In Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education (SIGCSE '17). ACM, New York, NY, USA, pp.225-230.

[6] Chothia, T., & Novakovic, C. (2015). An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15).

[7] List of CTFs Time. Available from: https://ctftime.org/

[8] M. Dark and J. Mirkovic, "Evaluation Theory and Practice Applied to Cybersecurity Education," in IEEE Security & Privacy, vol. 13, no. 2, pp. 75-80, Mar.-Apr. 2015.