An Effective Cybersecurity Exercises Platform CyExec and its Training Contents

Nobuaki Maki, Ryotaro Nakata, Shinichi Toyoda, Yosuke Kasai, Sanggyu Shin, and Yoichi Seto

***Abstract*—Recently the threats of cyberattacks, especially of targeted attacks are increasing rapidly and a large number of cybersecurity incidents are occurring frequently. On the other hand, capable personnel are greatly lacking, and strengthen the systematic human resource development cultivating capabilities for cybersecurity activities is becoming an urgent issue. However, only a few parts of academia and private sector in Japan can carry out the cybersecurity exercises because of high cost and inflexibility of commercial or existing training software. On this account, in order to enforce cybersecurity practical exercises cost-effectively and flexibly, we developed a virtual environment Cybersecurity Exercises (CyExec) system utilizing VirtualBox and Docker. We also implemented an open source vulnerability scanner tool WebGoat and our original cyberattack and defense training contents on CyExec.**

***Index Terms*—Cyberattack and defense exercise, cyber range exercise, ecosystem, human resource development on cybersecurity sector, threads, virtualization, vulnerability, WebGoat.**

I. Introduction

In this paper, we propose a cybersecurity exercises system in a virtual computer environment. This exercises system enables effective human resource development and contributes cybersecurity level of society. Backgrounds, characteristics, constitution and training contents of the exercises system are described below.

Cyberattacks are bringing serious social influences, causing vast cybersecurity incidents and even affecting business continuity. In January 2018, $530 million cryptocurrency was stolen in Japan, and in February 2018, organizations associated with the Pyeongchang Winter Olympics were targeted by cyberattack. These matters directly link to people's lives and cybersecurity is becoming a matter of deep social concern [1].

In the cybersecurity strategy of the Government of Japan, human resource development is cited as a serious issue. Human resource with skill insufficiency on cybersecurity is estimated at 190,000 by 2020 in Japan. The lack of technical knowledge and skill is worried even in personnel engaged in cybersecurity operations [2], [3].

As efforts towered human resource development and training for knowledge and skill regarding cybersecurity, some universities and public organizations are carrying out vulnerability learning exercises using dedicated software, and cyberattack and defense exercises using Cyber Range [4], [5].

Participants of the Cyber Range exercises learn practical defense technology against assumed cyberattack on the network in virtual environment. Participants also learn systematic correspondence method depending on roles in organization by using possible practical scenarios such as real malware infection. Therefore, high training effects can be expected [6].

However, universities have not enough exercises infrastructure to bring up cybersecurity human resources because of the high cost to introduce the practical exercises system and the lack of personnel to maintain the practice environment.

Therefore, a cybersecurity exercises platform which can promote joint development and common use is strongly required in the universities. This is the reason why we developed a cybersecurity exercises platform "Cybersecurity Exercises" (hereinafter referred to as CyExec) using a virtual computer environment of VirtualBox and Docker [7], [8].

Training contents implemented on CyExec is composed of a basic part and an applied part. Regarding the basic part, we implemented an open source vulnerability scanner tool WebGoat on CyExec and we developed a curriculum and a training guidance for the WebGoat exercises. Regarding the applied part, we developed and implemented our original cyberattack and defense training contents on CyExec.

In this paper, we describe the constitution of the cybersecurity exercises platform CyExec and training contents we implemented on it. We explain the outline of the cybersecurity exercises platform CyExec in Chapter II.; the problems and measures of training using open source vulnerability scanner tool WebGoat in Chapter III.; and the constitution of the training contents implemented on CyExec including WebGoat and our original cyberattack and defense training contents in Chapter IV.

II. Outline of the Cybersecurity Exercises Platform CyExec

A. Subjects of Existing Cyberattack and Defense Exercises

There are two kinds of existing cybersecurity exercises; using open source vulnerability scanner tool, and using commercial Cyber Range software.

1) Vulnerability scanning exercises

Vulnerability Scanning Exercises are aimed at learning the outline of the vulnerability, the detective method, and the

Manuscript received September 9, 2019; revised January 23, 2020.

Nobuaki Maki and Yoichi Seto are with Advanced Institute of Industrial Technology, Tokyo, Japan (e-mail: a1841nm@aiit.ac.jp).

Ryotaro Nakata is with Institute of Information Security, Yokohama City, Kanagawa, 221-0835, Japan.

Shinichi Toyoda and Yosuke Kasai were with Advanced Institute of Industrial Technology, Tokyo, Japan.

Sanggyu Shin is with Tokai University, Kanagawa, Japan.

countermeasures using open and free training software, such as WebGoat provided by OWASP (Open Web Application Security Project) [9].

Participants attending the lecture create the practice environment by installing the training software on their own PC and acquire diagnosis method and countermeasures against web application vulnerabilities systematically utilizing the software and the environment inside the PC.

However, training of correspondence method in organization is out of the scope from the vulnerability scanning exercises. In addition, the exercises are lacking interactive cyberattack and defense training and viewpoint of the exercises is limited to vulnerability detection and countermeasure on the static environment.

WebGoat is constantly revised in line with rapid technological changes, but only program materials are released. Therefore, frequent maintenance of the curriculum and the renewal of training guidance are necessary to correspond to the newest practice.

2) Cyber range exercises

Cyber Range exercises are aimed at upbringing of personnel available for responding to cybersecurity incidents in organization. The practice environment is constructed on a virtual environment imitating the real-world including clients, servers and network [10].

Trainees can learn attack techniques and knowledge of various types of malware, and train on confirmation of damaged situation and response method, assuming all stages of cybersecurity incidents recovery process from the beginning of the detection to the end of the response. The exercises are applicable to train personnel of Computer Security Incident Response Team (CSIRT) and Security Operation Center (SOC) [7], [8]. However, the introduction and operation of the Cyber Range exercises takes very high cost. In addition, the Cyber Range exercises are lacking the flexibility to change the curriculum in accordance with the intention of universities.

Universities need an exercises system to train the basics of vulnerability measures and response method in organization using the existing computer environment without adding anything. The vulnerability detecting exercises are suitable for learning the basics but are lacking the cyberattack and defense interactive training. On the other hand, the Cyber Range exercises are difficult to introduce in universities because of their limited budget and staff. For this reason, we developed the exercises system CyExec, described in the next section [7], [8], [11].

B. Characteristics of CyExec

CyExec is a cost-effective and flexible exercises system in a virtual environment to learn the basic technology of cyberattack and defense practically. It is expected to be introduced in universities and small and medium-sized enterprises. Characteristics of CyExec are shown below [7], [8].

1) Low cost and highly portable exercises environment

Most of the costs for installing and maintaining the cybersecurity exercises system are the costs of equipment and software licensing. To update the exercises system, personnel having specialized skills and high labor cost are required.

In order to reduce these costs, we developed an exercises environment using virtualization technology that can easily implement the training program in existing client and server computer environment. We utilized VirtualBox, which can operate a guest OS (virtual OS) on a host OS (Windows, macOS, etc.). On the virtual environment, we implemented the operating environment for the exercises program.

2) Practice environment for easy joint development and utilization

A high level of specialty and a long period of time are necessary for developing the cybersecurity training program. On the other hand, in the field of cybersecurity, technological progress is rapid. Therefore, it is difficult for a single university or private enterprise to develop a new cybersecurity training program and several organizations need to work together for the development. For this reason, we adopted the concept of ecosystem which will realize joint development and common utilization of the training programs between some organizations.

The word “ecosystem” means that whole associated organizations develop not on each single organization’s own but through the collaboration of related organizations. CyExec also enriches the training program not only by a single organization but also by joint development and utilize of related organizations [7], [8]. We have realized the joint development and utilization between multiple organizations by container technology using Docker.

We implemented Docker on the virtual environment constructed in VirtualBox, then we installed a container on Docker. It is easy for universities and private enterprises to build the training environment according to each purpose by implementing and operating various training programs on the container such as vulnerability diagnosis training or cyberattack and defense training. By making and releasing image files of the containers that operate the developed training programs, associated organizations can utilize them jointly.

The architecture of the CyExec system is shown in Fig. 1.

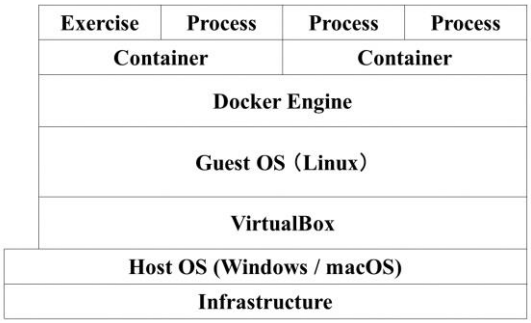

Fig. 1. The architecture of the CyExec system.

The architecture of the exercises system we developed has two-layer structure using Docker container. Docker is installed on the guest OS that operates on VirtualBox on the host OS. The processes, on which WebGoat and the cyberattack and defense training program run, is implemented on Docker container. VirtualBox has superior portability and Docker container has high extensibility for

any existing computer environment. They enable joint development and utilization of the training program.

III. Outline of WebGoat

A. Configuration of WebGoat Exercises

WebGoat is an open source software to teach web application security lessons designed and maintained by OWASP experts [9]. The detection method and countermeasures of vulnerability can be learned through the exercises.

As shown in Table I, WebGoat contains totaled 12 lesson plans and each lesson plan is consists of one or more subtopic.

TABLE I: Contents of WebGoat

No.	Category	Lesson Plan	Subtopic	Number of Assignments
1	Introduction	Introduction	WebGoat	0
			WebWolf	2
2	Basic Knowledge	General	HTTP Basics	2
			HTTP Proxies	1
			CIA triad	1
			Google Chrome Developer Tools	2
3		Injection Flaws	SQL Injection (introduction)	9
			SQL Injection (advanced)	3
			SQL Injection (mitigation)	3
			XXE	3
			Secure Passwords	3
4		Authentication Flaws	Authentication Bypasses	1
			Password reset	4
			Authentication Bypasses	1
			JWT tokens	4
5	Vulnerability Assessment	Cross-Site Scripting (XSS)	Cross Site Scripting	4
			Cross Site Scripting (stored)	1
			Cross Site Scripting (mitigation)	1
6		Access Control Flaws	Insecure Direct Object References	4
			Missing Function Level Access Control	2
7		Insecure Communication	Insecure Login	2
8		Insecure Deserialization	Insecure Deserialization	1
9		Request Forgeries	Cross-Site Request Forgeries	4
			Server-Side Request Forgery	2
10		Vulnerable Components	Vulnerable Components	2
11		Client side	Bypass front-end restrictions	2
			HTML tampering	1
			Client side filtering	2
12	CTF	Challenges	WebGoat Challenge	5

For example, summery of one lesson plan "Injection Flaws" is shown as bellow.

1) Subtopic

The lesson plan "Injection Flows" contains 4 subtopics: SQL Injection (introduction), SQL Injection (advanced), SQL Injection (mitigation), and XXE (XML eXternal Entity).

2) Contents

Each subtopic consists of some detailed contents: Explain the vulnerability; Assignments to learn about how to exploit the vulnerability; Describe the possible mitigation scenarios.

For example:

- SQL Injection (introduction): What is SQL, What is SQL Injection
- SQL Injection (advanced): Combining SQL Injection Techniques, Blind SQL Injection
- SQL Injection (mitigation): Defense against SQL,
- XXE (XML eXternal Entity): XML External Entity attack

3) Configuration

Each subtopic begins with Concept describing the explanatory policy, the Goal describing the achievement of the lesson, followed by the explanation of the vulnerability and some assignments that confirms the understanding.

B. Problems and Measures of Exercises Using WebGoat

1) Curriculum

The exercises theme of WebGoat consists of the latest technical issue selected by OWASP experts, but the learning level is unclear. Proper level setting is necessary for the exercises in the curriculum of universities in accordance with participants' practical skills and purpose of the training. See reference for details [11].

We adopted HMM (Hunting Maturity Model) proposed by Sqrrl, and SecBok (security knowledge field) human resource skill map published by JNSA (Japan Network Security Association) for the level setting [12], [13]. We matched the contents of WebGoat exercises with HMM level definitions and SecBok skill items.

The outline of the level setting is shown in Fig. 2. After clarifying the level setting, we developed the customizable curriculum using WebGoat.

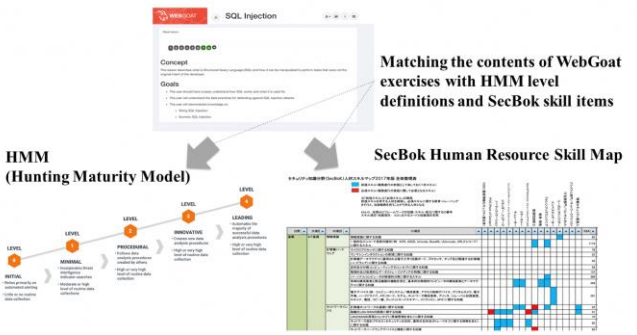

Fig. 2. Level setting t of the WebGoat exercises.

2) Training guidance for WebGoat exercises on CyExec

Description in WebGoat is written in cybersecurity professional style. In addition, prerequisite knowledge is necessary for many assignments in WebGoat. Therefore, a training guidance that explains the contents of WebGoat is required for lectures and trainees. For this purpose, we investigated the contents of WebGoat and created the training guidance.

IV. Development of Training Contents

A. Basic Concept

The training contents implemented on CyExec consist of a basic part and an applied part. Fig. 3 shows learning configuration of CyExec.

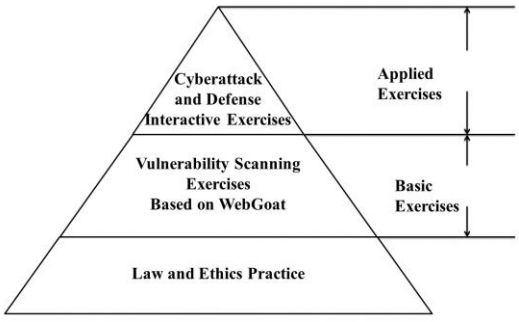

Fig. 3. Learning configuration of CyExec.

Regarding the basic exercises, we utilized the latest

version of WebGoat, v8.0.0.M25 [11]. We expect trainees to use inspection tools together such as OWASP ZAP (OWASP Zed Attack Proxy) to detect vulnerabilities [14].

WebGoat exercises are developed based on OWASP experts' technical regular research on high risk vulnerabilities, therefore the basic exercises have high training effects.

Regarding the applied exercises, we constructed interactive environment of attacker and defender to realize practical exercises. Fig. 4 shows an example of the applied exercises environment.

The environment for the attack defense training is constructed using Docker on a virtual guest OS in a closed network separated from the outside. Both of the attacker's and the defender's practice environments are built on the Docker container. The trainees playing the role of the attacker exploit vulnerabilities from the attacker's environment and the trainees playing the role of defender monitor the network traffic and analyze the log regarding the cyberattack in the defender's environment.

High expertise and a long periods of time are required to develop the new cyberattack training contents by a single organization. CyExec enables joint development of the training contents in short time by cooperation of multiple universities and private enterprises [7], [8].

In addition to the basic exercises and the applied exercises, we also focused on law and ethics practice before the exercises to prevent participants from illegal and injustice use of acquired skill by intention or fault.

We expect active learning where participants are engaged in solving problems, learn lessons at home using a training guidance in advance and exercises with a lecturer's help after learning the necessary skills.

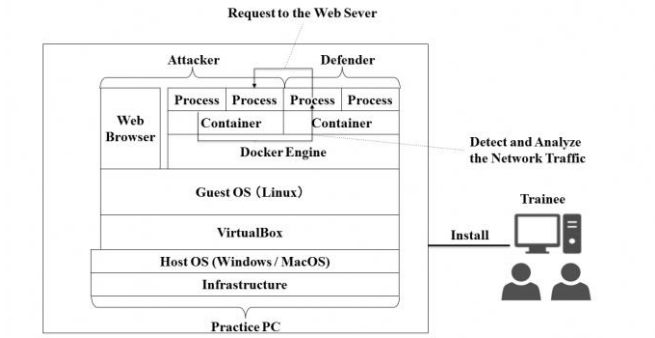

Fig. 4. Example of environment of the configuration of CyExec applied exercises.

B. Basic Exercises Using WebGoat

The basic part of CyExec is exercises to learn about the outline of vulnerability, detection and countermeasure. We selected themes of the basic exercises considering the priority of vulnerabilities shown in OWASP Top 10 and the suitability for the curriculums in the universities [15]. OWASP Top 10 is the 10 most seen application vulnerabilities and their detection and prevention methods updated regularly by experts in OWASP project, and becomes widely used around the world. Table II shows the correspondence between the CyExec theme and OWASP Top 10.

We defined the learning level and skills for each selected exercises theme using HMM and SecBok described in Chapter 3.

TABLE II: CORRESPONDENCE BETWEEN WEBGOAT AND OWASP TOP10

	Category	Lesson Plan	OWASP Top 10
1	Introduction	Introduction	-
2	Basic Knowledge	General	-
3	Vulnerability Assessment	Injection Flaws	A1:2017-Injection A4:2017-XML External Entities (XML)
4		Authentication Flaws	A2:2017-Broken Authentication
5		Cross-Site Scripting (XSS)	A7:2017-Cross-Site Scripting (XSS)
6		Access Control Flaws	A5:2017-Broken Access Control
7		Insecure Communication	-
8		Insecure Deserialization	A8:2017-Insecure Deserialization
9		Request Forgeries	A8:2013–Cross-Site Request Forgery (CSRF)
10		Vulnerable Components	A9:2017-Using Components with Known Vulnerabilities
11		Client side	-
12	CTF	Challenges	-

For example, summery of "SQL Injection" exercises is shown as bellow.

1) Purpose of the exercises

Purpose of the basic exercises is to understand basic knowledge of SQL, outline of SQL injection and detection method and to acquire basic skills on cyberattack and defense through assignments.

2) Capable skills of being acquired

The following are example of learnable skills. These items are selected from the SecBok skill table described in Section III. *B.*

- Basic knowledge of vulnerability assessments
- Knowledge of system and application security threats and vulnerabilities
- Skill in recognizing and categorizing types of vulnerabilities and associated attacks

3) Basic knowledge of SQL

SQL (Structured Query Language) is a language for data definition, data control, and data manipulation. It enables accessing and updating records of a database.

SQL consists of three types of statements:

Data Manipulation Language (DML): SELECT, INSERT, UPDATE, DELETE

Data Definition Language (DDL): CREATE, ALTER, DROP, TRUNCATE

Data Control Language (DCL): GRANT, REVOKE

4) Outline of SQL injection

SQL injection is code injection technique using vulnerability which allows an application to execute an unintended malicious SQL statements inserted into request of an entry field to manipulate the database improperly. Exploiting this vulnerability causes falsification and leakage of data in the database.

5) Harmful effects of SQL injection

SQL injection induces disclosure or destruction of the confidential data, improper program execution and file reference, and theft of database server administrator authority.

6) Attack example

An overflow of a literal (a constant in the SQL statement) causes the SQL injection. The following is an attack example using the vulnerability.

"select * from users where name='"+username+"'"; (1)

The variable userName in Statement (1) stores the input value received from the request. For example, when the attacker supplies unexpected string "Smith' or '1'='1" in the variable userName, the range of the SQL literal becomes to be "name='Smith'" and the part of "or '1'='1'" is pushed out and executed. Since "or '1'='1'" is always true, information that does not match the condition leaks.

7) Assignments

Fig. 5 shows an example of SQL Injection assignments.

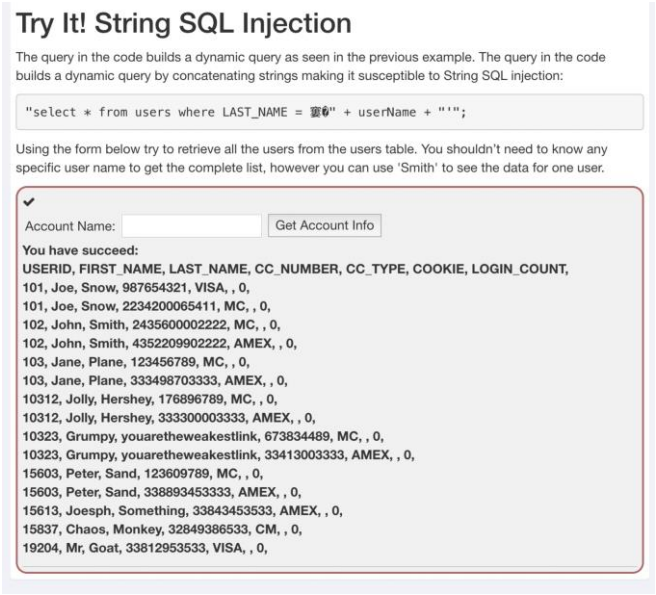

Fig. 5. Example of assignments about string type SQL injection.

Trainees try to acquire and display the user information from the database exploiting the vulnerability of the SQL injection without access permission.

C. Applied Exercises Using Original Cyberattack and Defense Program

After learning the basics of vulnerability and countermeasures in the basic exercise CyExec provides the applied exercises to offer more practical cyberattack and defense techniques. Trainees can improve the response ability in organization against various kind of cyberattacks through the applied exercises simulating the different roles and viewpoints such as attacker and defender, manager and general user.

The exercises are carried out separately in the attacker's side and the defender's side. The outline of the applied exercises is described below.

1) Purpose of the exercises

The purpose of the exercises is to acquire cyberattack and defense skill comprehensively from the following viewpoints. Purpose of training attack skill is limited only to deep understandings of defense technology.

- To understand cyberattack methods exploiting vulnerabilities: Vulnerability detection using tools such as OWASP ZAP, attacks exploiting vulnerabilities of software or server
- To understand defending methods against cyberattacks: detection and analysis of cyberattacks using access log file, countermeasures against cyberattacks

2) Capable skills of being acquired

Examples of specific learnable skills are as following.

- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data
- Knowledge of penetration testing principles, tools, and techniques
- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
- Skill in using network analysis tools to identify vulnerabilities

3) Configuration of exercises system

Fig. 6 shows an outline of configuration of the exercises system.

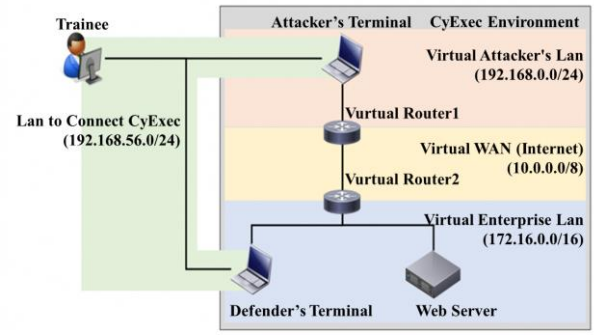

Fig. 6. Configuration of exercises system.

The trainees exercise after logging in either attacking terminal or defensing terminal operating on the Docker container on CyExec. Two terminals communicate each other through a virtual network constructed on the Docker container.

The attacker operating the attacking terminal exploits vulnerability, logs in the defending web server via virtual network without proper authorization, and attempts to infect the server with an attack script. The main goal for the attacker is to steal confidential information using the script.

The defender tries to find the sign of the attack by monitoring the network traffic logs from the attacker. The main goal for the defender is to consider the attacks, to implement countermeasures and to ensure that the attacks can be prevented.

4) Program specification

The specifications of the exercises program are shown below.

a) Guest OS

- OS: Ubuntu 18.04
- Memory: 2GB
- Storage: 20GB
- Container platform: Docker 18.09

b) Exercises program

- Programming language: Ruby 2.5.1, PHP 7.2
- Database management system: MySQL 8.0
- Web server software: Apache 2.4

c) Software development process model

We adopted the spiral development model. The development period was divided into several phases to develop and improve the exercises program at the proper time.

We promoted the development efficiently by using Docker Hub to share the created containers on the cloud, and GitHub to manage source code versions.

d) Development man-month

Approximately 6 man-month

5) Exercises scenario

Fig. 7 shows the image of the exercises scenario.

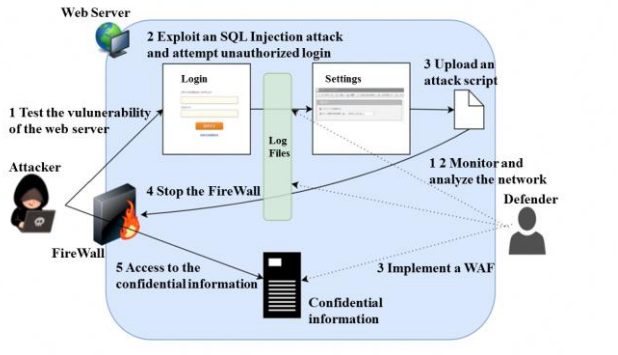

Fig. 7. Image of the exercises scenario.

a) Scenario of the attacker

The contents of the exercises of the attacker are shown below.

1) Test the vulnerability of the web server using OWASP ZAP and make a report of inspection results.
2) Exploit an SQL injection attack on the vulnerable web application and attempt unauthorized login.
3) Upload an attack script using the file upload function after login.
4) Access to and execute the attack script from the browser on the attacker's terminal and execute the script to stop the firewall using the attack script.
5) Unauthorized access to the confidential information in the web server using SSH command.

b) Scenario of the defender

The contents of the exercises of the defender are shown below.

1) Monitor the network log from the attacker using tools such as Apache Log Analyzer to detect the SQL injection attack and the attack script.
2) Modify source code causing SQL injection vulnerability and confirm the improvement.
3) Implement a Web Application Firewall (WAF) and confirm that WAF can prevent the unauthorized access to the confidential information on the Web server.

V. Conclusion

Cyberattacks including targeted attacks are increasing and becoming serious issues of digital society. Enforcement of the human resource development for personnel having cyberattack and defense skills is an urgent priority, but the environment for growing up the cyber security personnel is still poor because of the high cost of the exercises system and the shortage of the personnel to maintain and manage the exercises environment.

Therefore, we developed a cybersecurity exercises system CyExec consisting of virtual environments using VirtualBox and Docker container based on ecosystem.

The basic contents on CyExec are using open source vulnerability scanning tool WebGoat. The applied contents on CyExec are our original cyberattack and defense exercises programs.

In this paper, we introduced the contents of the vulnerability diagnosis exercise using WebGoat implemented in CyExec and the cyberattack and defense exercises program we developed.

In the future, we plan to develop and utilize CyExec with other universities and small and medium-sized enterprises jointly.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

RN, SS and YS conceived of the presented idea; ST, YK, SS and YS developed the theory and implemented the exercises contents; NM, SS and YS wrote the paper; YS supervises the findings of this work; all authors had approved the final version.

Acknowledgment

This work was supported by JSPS KAKENHI Grant number JP 19K03006. This study was supported in part by Research and Study Project of Tokai University Educational System General Research Organization.

References

[1] Information-technology Promotion Agency, *Japan: Information and Security White Paper 2018 (in Japanese)*, 2018.
[2] National Center of Incident and Strategy for Cybersecurity, Japan: Cybersecurity Strategy. (2018). [Online]. Available: https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugiketteai.pdf
[3] Ministry of Economy, Trade and Industry. (2016). Japan: Survey on latest trends and future estimates of IT personnel (in Japanese). [Online]. Available: http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf
[4] National Institute of Information and Communications Technology: Practical cyber defense exercises Cyder (in Japanese). [Online]. Available: https://www.nict.go.jp/press/2019/03/20-1.html
[5] K. Nakajima *et al*., "Proposal of an environment for practical system security learning from the viewpoint of "Hacker"," presented at the 30th Annual Conference of Japan Society for Software Science and Technology, Tokyo, 2013.
[6] M. Edure, "Practical exercises for cyberattack (in Japanese)," *IPSJ Magazine*, vol. 55, no. 7, 2014.
[7] S. Toyoda *et al*., "Proposal of cyber attack and defense exercise system CyExec composed of ecosystem (in Japanese)," *Computer Security Symposium*, Nagano, 2018.
[8] Y. Kasai, Y. Seto *et al*., "Development of practice contents for cyber security exercise system CyExec (in Japanese)," presented at Symposium on Cryptography and Information Security, Otsu, 2019.
[9] OWASP WebGoat Project Homepage. [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
[10] LAC Co., Ltd., "Current status and trends of information security - Implementation procedure and practice case of cyber exercises - (in Japanese)," 2015.
[11] WebGoat new releases homepage. [Online]. Available: https://github.com/WebGoat/WebGoat/releases
[12] R. Nakata *et al*., "Container-type virtual exercise system CyExec for cyberattack and defense (in Japanese)," presented at the 80th National Convention of Information Processing Society of Japan, Tokyo, 2018.

[13] Japan Network Security Association, SecBok Human Resources Skill Map (in Japanese), 2017.
[14] OWASP Zed Attack Proxy Project Homepage. [Online]. Available: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
[15] OWASP Top Ten Project Homepage. [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Nobuaki Maki was born in Tokyo, Japan in 1972. He received the B.Sc. in physics from Kyoto University, Kyoto, Japan, in 1996. Since 2018, he has been enrolled in the master course of Advanced Institute of Industrial Technology, Tokyo, Japan.

In 1998, he joined the Ministry of Health Labour and Welfare, Government of Japan. In 2012, he became First Secretary, Embassy of Japan in Indonesia. In 2015, he became Deputy Director, Overseas Cooperation Division, Human Resource Development Bureau, Ministry of Health Labour and Welfare. Since 2016, he has been Cyber Security Officer, Compensation Operation Division, Labour Standards Bureau, Ministry of Health Labour and Welfare.