International Journal of Learning Technologies and Learning Environments
International Institute of Applied Informatics
2020, Vo. 3, No. 1, 1 – 20

CyExec - Training Platform for Cybersecurity Education Based on a Virtual Environment

Sanggyu Shin *, Yoichi Seto †

Abstract

In this paper, we propose the CyExec, an effective cybersecurity training platform in a virtual computer environment. Recently the threats of cyberattacks, especially of targeted attacks, are increasing rapidly, and a large number of cybersecurity incidents are frequently occurring. On the other hand, capable personnel is much lacking, becoming an urgent issue that strengthens the systematic human resource development cultivating capabilities for cybersecurity activities. Only a few parts of universities and companies in Japan are conducting education using an effective training system on the market because of expensive and difficult to use that adopted and operation the training system like Cyber Range in higher education institutions and SMEs. On this account, we developed a virtual environment named Cyber Security Exercises (CyExec) system utilizing VirtualBox and Docker to enforce practical cybersecurity exercises cost-effectively and flexibly. In our proposal, we imported the implementation of the OSS vulnerability diagnosis in our system, and developed and implemented a cyberattack and defense training program based on the WebGoat that cybersecurity training system program.

Keywords: cybersecurity, education, training platform, CyExec.

1 Introduction

In this paper, we propose a cybersecurity exercise system and its exercise contents in a virtual computer environment based on Virtualbox and Docker. We anticipate this exercise system enables active human resource development and contributes cybersecurity level of society [1]. We describe below the backgrounds, characteristics, constitution, and training contents of our proposal exercises system.

Increasing of incidents on the virtual environment by cyberattacks cause social impacts such as affecting business continuity has become apparent. Even in Japan, incidents directly related to daily life occur now and then, like the information leakage incident of the Japan Pension Service of May 2015. Also, in January 2018, $530 million cryptocurrencies were stolen in Japan, and in February 2018, the cyberattack targeted the organizations associated with the Pyeongchang Winter Olympics. These accidents directly linked to the lives of people, and for these reasons, the social concerns and needs for cybersecurity are

* Tokai University, Kanagawa, Japan
† Advanced Institute for Industrial Technology, Tokyo, Japan

increasing [2]. Human resource development is citing as an essential issue in the cybersecurity strategy of the government. In Japan, the insufficiency of human resources has skilled in cybersecurity is estimated at 190,000 by 2020 [3][4]. 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. A Cyber Range is a virtual environment that trains vulnerability exercises using specific applications and tasks. In Japan, at the public institution such as the NISC (National Center of Incident readiness and Strategy for Cybersecurity) and NICT (National Institute of Information and Communications Technology), there are lectures by specialist organizations as examples of the efforts to develop human resources at a civil servant [5][6][7].

CYDER (CYber Defense Exercise with Recurrence), which is a practical cyber defense training exercise for government agencies and essential infrastructure operator, has been increasing in number each year and expanded from 2018 [8]. Participants of the Cyber Range exercises learn practical defense technology against an assumed cyberattack on the network in a virtual environment. In this closed network environment, participants also learn the systematic correspondence method depending on roles in the organization by using possible practical scenarios such as real malware infection. Therefore, participants can expect high training effects [9]. However, higher education institutions such as technical colleges and universities do not have enough exercise infrastructure to bring up human resources at the heart of cybersecurity because of the high cost of introducing the practical exercises system and the lack of personnel to maintain the training environment.

To solve these problems, required the ecosystem strongly in the higher education institutions and small and medium-sized enterprises. In this paper, the ecosystem means a cybersecurity exercise platform that can promote joint development and joint use. This demand is the reason why we developed a cybersecurity exercise platform, Cybersecurity Exercises (from now on referred to as CyExec), using a virtual computer environment based on VirtualBox and Docker [10]. The exercise contents implemented on CyExec is composed of a "Basic Part" and an "Applied Part." Regarding the basic part, we were porting an open-source vulnerability scanner tool WebGoat on CyExec and developed a curriculum and training guidance for the WebGoat exercises. Regarding the applied part, we developed and implemented cyberattack and defense training contents on CyExec, to possibly experience a possible cyberattack and defense side.

In this paper, we describe the constitution of the cybersecurity exercises platform CyExec and the training contents we implemented on it. In Chapter 2, we discuss the issues in constructing the training environment. Introduces an overview of the CyExec that cybersecurity exercise system in Chapter 3. In Chapter 4, we discuss the problems and countermeasures of the WebGoat, which is the vulnerability diagnosis learning program, and Chapter 5 we introduce the development of exercise content.

2 Issues in Constructing the Training Environment

2.1 Survey on How Training is Being Conducted

We investigated the contents/courses of cyber attacking and defense exercises in educational institutes such as universities or specialized institutions, at present status, to raise the security personnel resources. The survey method was conducted by interviewing six organizations and others, including public information, questionnaire surveys by concerned

parties, and participating in exercises [7][8]. Table 1 shows the target organizations and a brief of their training. Based on the survey, we divided the exercises into the following two forms.

(1) Exercises by the learning applications

(2) Exercises by the Cyber Range

We confirmed the main contents of each type.

Table 1: Contents of the exercise and training to raise the security personnel resources

Name	Overview
Tokyo Institute of Technology	Five courses are offered from 2016 as an own cybersecurity specialized study program. Exercise subjects are assigned by external lecturers from cooperating companies. Training focuses on how to use tools and OWASP applications etc.
Institute of Information Security	Introduced a large-scale exercise system, operated in cooperation with companies. Mastering a wide range of practical security skills through exercises, from technical subjects to social science subjects, towards multi-talent security human resources.
enPiT	Covering a wide range of practical security skills, from technical entity to social science subject, toward the training of human security resources sought by industry. Learning security practical skills in various forms such as learning using learning applications, collective exercises, group exercises.
Tokyo Denki University	International Cyber Security Special Course “CySec” started in 2015. For the graduate students and people aiming to become senior security engineers or CISO engineers. Practice exercises on security technology, attack countermeasure, and network design.
The university of AIZU	Intensive lecture for information security engineers “Cyber-attack countermeasure exercise” was implemented from 2014. Using a large-scale exercise system in cyber-attack/defence exercises. The external corporate lecturer is in charge of cyber-attack outlines and exercises part. Implementation of practical scenario exercises from security techniques and application of tools and others.
NICT (National Institute of Information and Communications Technology)	Developed and implemented practical cyber defence exercises from 2016 for administrative agencies, local governments, independent administrative agencies, and important social infrastructure operators in the country as stipulated in the Cyber Security Basic Law. Practical exercises by constructing a virtual exercise environment at NICT “StarBED.”

2.1.1 Exercise by the learning application

The exercises by learning applications are installed on desktops or servers and help to learn about vulnerabilities, attack methods, and countermeasures (defense methods). Typical examples are WebGoat provided by OWASP (Open Web Application Security Project) and AppGoat supplied by IPA (Information-technology Promotion Agency, Japan), which are available for free [11][12][13].

The WebGoat is an application that learns about various vulnerabilities by learning how to do the tasks while practicing them and learning about 20 vulnerabilities such as XSS (Cross-Site Scripting) and SQL injection. It is possible to improve understanding of the attack mechanism by making it easier for beginners to learn how to use it, such as providing tutorials and hints step by step [14]. However, there are no explanations about the impacts of the attack, and there are insufficient practical parts such as judgment on the danger and extent of influence, decision on the presence or absence of an attack. The WebGoat can be freely downloaded and used. But, in addition to providing the English version only, the content update depends on the OWASP provider.

The AppGoat can train interactively about conducting explorations of vulnerabilities, grasping problems on the code, and learning countermeasures against exercises prepared for each learning theme. The tools are divided depending on the target and application. There are tools for learning about 12 vulnerabilities for website administrators and web application developers, and tools for learning about 7 vulnerabilities for server and desktop application developers. The tool for web application developers can be used for collective learning such as lectures and seminars as well as functions for grasping learners' abilities and for simultaneous use by multiple users. The AppGoat requires a subscription to the IPA, but it provides more detailed explanations of attacks than the WebGoat and touches on impacts and countermeasures. Also, in the collective learning mode, preparations for the exercises, how to proceed, and supplementary materials that can be used in the exercises are provided. In this way, the burden on the instructor is reduced, and the exercises can be practiced [14].

However, like WebGoat, these learning applications are primarily aimed at understanding the content of vulnerabilities and threats, and, of course, there are some areas where they can learn about countermeasures. However, in practice, it is not enough to acquire practical knowledge, such as knowledge and skills required for actual work.

2.1.2 Exercises by the Cyber Range

The Cyber Range exercises create an environment simulating the real world, such as servers, clients, and networks, in virtual environments, and prepare security devices that are used. Exercises will be implemented in actual scenarios, for instance, inducing incidents using an unauthorized program of attacks, such as real malware, in the same environment as in the real world. For example, dynamic exercises may be carried out by changing the content of an attack depending on the participants. It is also possible to combine the knowledge and skills required for security work, such as attack methods and types of malware, that practical exercises will implement [15].

In the case of conducting the Cyber Range exercise, it is necessary to purchase a system provided by a private company, install and maintain the equipment, examine the training courses, and prepare the environment. In addition to the cost of the software and hardware,

the economic burden is substantial because it implies human resources to manage the system. For this reason, it is difficult for the organization to establish a realistic environment for exercises, and it is operated in cooperation with private companies.

Moreover, research on the exercise system itself has been conducted [16][17]. CyTrONE is a system that realizes the automation of the virtual environment construction required for the exercises, which is being studied and provided in the JAIST (Japan Advanced Institute of Science and Technology). By installing the prepared configuration file, the preparation work can be significantly reduced by constructing an exercise environment with only tens of minutes. However, to operate CyTrONE, it is necessary to prepare a specific system environment, and the scenario of the exercise needs to be developed separately by the teacher [18].

2.2 Issues and requirements of the exercises

To examine the exercise system, which can be introduced by many educational institutions, we confirmed the problem of the implementation of the actual exercise. Table 2 lists the advantages and disadvantages of existing exercise systems.

From Table 2, the existing exercise system has features related to exercise scenarios such as introduction and preparation of equipment to conduct exercises, features described to use environments, and examination, update, and the addition of contents to be learned.

Table 2: Features of existing exercise system

Exercise type	Merit	Disadvantage
Learning by application for exercise Example: WebGoat (OWASP) AppGoat(IPA)	1. Can practice at low cost. 2. Easy preparation of the environment. 3. Possible to use it on an individually.	1. Exercise content is fixed. 2. Development and updating depend on the provider; there may be cases where a learner cannot practice according to a purpose.
Exercise by Cyber Range Example: CYBERIUM (Fujitsu) TAME Range (DNP) CyTrONE (JAIST)	1. Practical and useful exercises are possible because it uses realistic scenarios. 2. By changing the scenario, can respond to exercises of various contents.	1. System installation and maintenance cost is very high. 2. Human resources with expertise and corporate cooperation are necessary for environmental improvement and scenario development.

Regarding the exercise environment, a particular system environment is necessary for practical and useful exercises, and a collaborative system of experts and companies is indispensable.

Regarding the exercise scenario, it is required to concretize the latest vulnerabilities and threat trends into practical exercises, including countermeasures, but it is not easy for the teacher to prepare scenarios according to various objects and purposes. We need to review

the details of these issues and examine the exercise system that can be introduced by many organizations.

2.2.1 Exercise environment

To implement cyber-attack/defense exercises, it is challenging to introduce it in many organizations because the following requirements are necessary.

- Introduction and maintenance of the system environment required for the implementation of the exercise
- Secure experts and operators with knowledge for exercises

Exercises using learning applications do not require a particular exercise environment and can be prepared relatively quickly, so it is assumed that many educational institutions will introduce them. However, it is necessary to conduct exercises with the existing personnel structure. For example, at the university, the faculty members must make it possible to perform activities with information without adopting newly specialized faculty members.

Exercises by Cyber Range will construct an environment equivalent to the real world using a large-scale system (server, network equipment, security equipment, and software) for building the exercise environment. In addition to expensive installation costs and maintenance costs, it is necessary to secure expenses and personnel aspects such as personnel and expertise with expert knowledge on conservation and setting. However, it is not easy to ensure the costs and specialized staff at educational institutions such as universities and small and medium enterprises, etc. Thus it is difficult to prepare the exercise environment without financial margin or support of enterprises.

Therefore, it is necessary to have an exercise environment that can be introduced at a low cost and can be introduced and maintained with existing personnel.

2.2.2 Exercise scenarios

When considering the exercise scenario, it is necessary to discuss the following contents; it is challenging to respond only by a teacher who does not have expertise.

- New content including new attack methods and vulnerability information
- Confirm the skills that students should learn
- Effective learning content for acquiring skills

Vulnerability information on systems and applications is updated daily. Cyber-attacks using them are increasing, and more and more advanced all over the world. Fortunately, defense technology is evolving too. Therefore, it is necessary to understand the current situation, check whether the content dealt with in the exercise is appropriate, and add or change the content of the study.

Also, the users are diverse, like students, IT engineers, security workers, and others. The content and level of the skill to be learned changes by the user level of expertise, so it is necessary to confirm the required skills for each student.

When training, users exercise attack and defense behavior according to the scenario and acquire skills in exercise. In learning applications, the user can learn skills about essential contents cross-cuttingly because of learning the materials prepared in advance. Cyber

Range training is carried out assuming scenarios of attack and defense, which can occur in reality considering the actions of the attacking side, the defending team, the technology used, the type of malware, the environment, etc. Therefore, we need to consider various contents, such as finding attack and defense techniques and handling tools to be used according to the students.

The development of the exercise scenario requires expertise in security and familiarity with the target device/system. In some cases, growth is entrusted to companies, and additional costs are also needed in addition to environmental improvement.

In the curriculum, to conduct exercises widely at educational institutions and small and medium enterprises, it is necessary to develop a scenario suitable for the students. Still, it is difficult for teaching members who do not have expertise in security to deal with it. Also, in university lessons, a practical curriculum including a plurality of exercises and accompanying learning contents is necessary, and preparation requires a particular technique and time.

Therefore, it is necessary to establish a method by which the teacher can do the scenario set so that you can grasp the required skills and learn them. Also, a system of joint development and mutual use by multiple educational institutions is more effective.

3 Outline of the CyExec - Cybersecurity Exercises Platform

3.1 Issues of cyber attack and defense exercises

There are vulnerability diagnosis and Cyber Range as usual practice methods about cybersecurity. In this chapter, we introduce each feature briefly.

3.1.1 Vulnerability Assessment Exercise

Learners could learn about the outline of vulnerability, detection method, and measures using OSS. Some organizations are providing a free version exercise program. For example, there are WebGoat provided by OWASP and AppGoat provided by IPA [11][12]. These vulnerability assessment exercises can build an exercise environment by installing the exercise program on the learner's PC.

Learners can use these exercise programs to acquire vulnerability assessments and countermeasures systematically for web applications. In the vulnerability assessment exercises, organizational measures are outside the scope of learning. It also lacks interactive activities divided into attack and defense and is limited to static vulnerability detection and countermeasures.

Although the AppGoat has a curriculum designed for group education like a class in univ., it is inflexible because challenging to change the curriculum. WebGoat is providing exercise programs only, although program revisions are being conducted at set in line with technological changes. Therefore, to use in university requires the maintenance of a curriculum, and a text for exercise is necessary.

3.1.2 Exercise on Cyber Range

This exercise is aimed to bring up organizational personnel able to respond to security incidents. The exercise environment is constructed on the virtual environment by imitating the real world, such as client, server, and network [19].

The learner can learn from attacks to the response to these attacks, such as attack methods, types of malware, confirmation of damage situation, and training on response methods, against attacks using malicious programs such as malware. Cyber Range responds to human resource development such as Computer Security Incident Response Team (CSIRT) and Security Operation Center (SOC). However, the Cyber Range is expensive to build and operate. It also lacks the flexibility to change the curriculum according to the intention of the higher education institution.

Higher education institutions need an exercise system that can learn the basics of vulnerability measures and systematical responses using the existing computer environment. Vulnerability diagnosis is suitable for learning the basics but lacks the interactivity of attack and defense.

On the other hand, the Cyber Range is challenging to build in higher education institutions with limited budget and personnel. We developed the exercise system CyExec described in the next section [20].

3.2 Features of CyExec

The goal of CyExec is to provide an exercise system that learns the necessary technology of cyber attacks and defense intended for introduction in higher education institutions and small and medium enterprises [20]. We show the features of the CyExec below.

3.2.1 Low cost, highly portable exercise environment

Most of the costs of building and maintaining the exercise system are the cost of equipment and the cost of licensing software. To renewal the exercise, the system requires personnel with specialized skills, and the price such as labor cost is substantial.

To reduce these costs, we built an exercise environment using virtualization technology to quickly implement the developed exercise program in an existing computer environment (client PC, server, etc.). Using VirtualBox, we implemented the exercise program operating environment in a virtual environment.

3.2.2 Exercise environment to secure joint development and use

The development of the training program requires a high level of expertise and time, and also advances in the security technology field rapidly change. For these reasons, it is challenging to complete the exercise program development at a single higher education institution. Therefore, it needs to work together to develop practice programs that several higher education institutions and private companies. We realize joint development and the use of exercise programs in multiple organizations by introducing the ecosystem concept.

The ecosystem is not a single organization, but a word that indicates that the whole related organization develops through the collaboration of associated organizations. CyExec enriches the exercise program of CyExec not only by a single organization but also by joint development and use of related organizations.

For the training system, to realize joint development and utilization by multiple higher education institutions, it is necessary to develop and utilize exercise programs among different institutions quickly. To achieve this request, we implemented by container technology using Docker.

We implemented Docker on the virtual environment configured with VirtualBox and install a container on Docker. By implementing vulnerability assessments and various exercise programs on attacks and defenses and running them on a Docker container, we could easily construct a practice environment for each purpose. It can also be used jointly by creating an image file of a container that runs the developed exercise program and publishing it in related organizations. Table 3 shows the comparison of CyExec and other exercise systems.

Table 3: The comparison of CyExec and other exercise systems

	Exercise system example (Developer)		
	Proposed exercise system CyExec	WebGoat (OWASP), AppGoat (IPA)	CYBERIUM (Fujitsu), TAME Range (DNP)
Cost	Program, text development free	Text development cost	Expensive system introduction operation cost
Exercise form	• Individual learning / Large-scale exercise • Operation of other exercise systems is also possible	Individual learning/Small exercise	Large scale exercise
Exercise content	• Can learn from the fundamentals of vulnerability detection to an organizational response method • Customizable according to study purpose	• Fixed exercise content • Update depends on the developer • Practice exercises concerning commentary/usage guides	• Personnel with expertise is required for operation • Update by development/provider (paid)
Feature	• High portability/extensibility with the ecosystem as a development concept • Improvement of the appropriate curriculum by cooperative development	• It can be carried out on student PCs and can be used on their own • Easy to introduce practical environment • Supplementary text required	• Exercise imitating the real environment • Practical exercises using actual malware

Figure 1 shows the architecture of the CyExec exercise system. The architecture of the exercise system developed is to install Docker on the guest OS running on VirtualBox on the host OS, and implement the process on which the attack and defense exercise program runs on the container on Docker. The portability that can operate in the existing computer environment of VirtualBox and the high extensibility of the Docker container enable joint development and use of our exercise program.

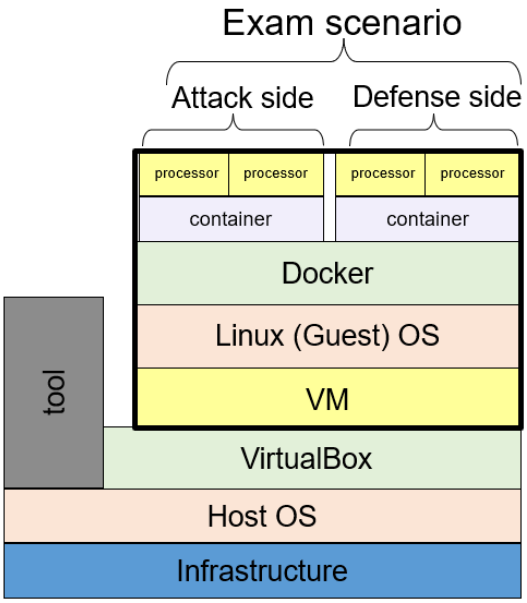

Figure 1: The architecture of the CyExec exercise system

4 Issues and Measures of Exercises Using WebGoat

WebGoat is an OSS vulnerability diagnosis training program that developed and published by experts of the OWASP community. Through exercises aimed at Web applications, a learner can learn about the outline of vulnerability, detection, countermeasures, etc.. As shown in Table 4, there are a total of 12 exercise themes targeted by WebGoat.

The WebGoat exercises consist of experts compiled with the latest technical content, but the level of learning to correspond to the learner is not clearly indicated. When conducting exercises using a curriculum at a higher education institution, it is necessary to set levels by practical skills and educational standards. Reference the details at [21]. The setting of the study level uses HMM (Hunting Maturity Model) proposed by Sqrrl, and the SecBok (security knowledge field) human resource skill map published by JNSA (Japan Network Security Association) [22][23] . We corresponded to the WebGoat exercises to the HMM level definitions and the SecBok skill items. For study level setting, after clarifying how to set the learning level, we developed a curriculum with which can customize the content of exercises using the WebGoat.

WebGoat documents for experts is written in English. Besides, there may be cases where prerequisite knowledge is required to carry out the exercises. Therefore, to be used by lecturers and learners at higher education institutions, documents that explain the contents of WebGoat's tasks are required. For this purpose, we investigated and translated the materials of WebGoat's exercises and created documents.

Table 4: Learning content 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
			HTTP CLA triad	1
			Google Chrome Developer Tools	2
3	Vulnerability diagnosis	Injection Flaws	SQL Injection (introduction)	9
			SQL Injection (advanced)	3
			SQL Injection (mitigation)	3
			XXE	3
			Secure Passwords	3
4		Athentication Flaws	Authentication Bypasses	1
			JWM tokens	4
			Password reset	4
5		Gross-Site Scription (XSS)	Cross Site Scription	4
			Cross Site Scription (stored)	5
			Cross Site Scription (mitigation)	4
6		Access Control Flaws	Insecure Direct Object References	4
			Missing Function Level Access Control	2
7		Insecure Communication	Insecure Login	1
8		Insecure Deserialization	Insecure Deserialization	1
9		Request Forgeries	Cross-Site Request Forgeries	4
			Server-Side Request Forgery	2
10		Vulnerable Comonents	Vulnerable Components	2
11		Client side	Bypass front-end restrictions	2
			Client side filtering	2
			HTML tampering	1
12	CTF	Challenges	WebGoat Challenge	5

5 Development of Exercise Content

5.1 Base Concept

The exercises implemented to CyExec consist of the "Basic exercises" and the "Applied exercises." Figure 2 shows the content of the training of CyExec.

	Security Assessment testing	Cyber Range
Target	• Web application vulnerability	• Security equipment • Incident response officer
Contents	• Vulnerability Principles, Detection, Impact and Measures	• Security vulnerability response • Interactive attack and defense technology • Organizational response when an incident occurs

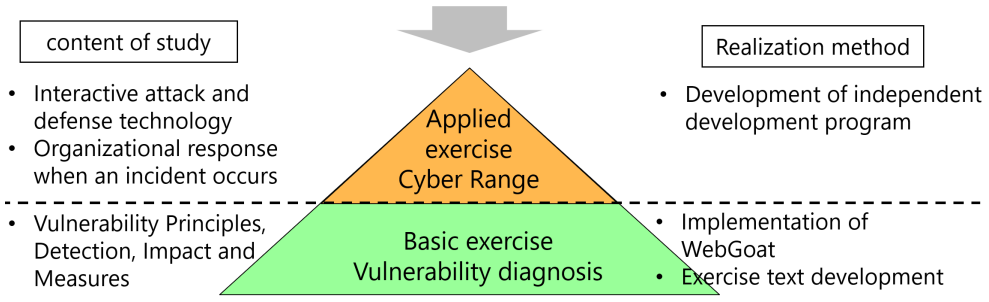

Figure 2: Learning range of CyExec

In the basic exercises, learners learn based on WebGoat. The version of WebGoat adopted the v8.0.0.M21. The learner uses an inspection tool such as OWASP ZAP (OWASP Zed Attack Proxy) to detect vulnerabilities, etc. [24].

WebGoat is developing by experts regularly about summarizing the key points and developing exercises on high-risk vulnerabilities. Therefore, high educational effects can be expected. Application part exercises carry out practical tasks in an interactive environment of attack and defense.

An interactive exercise environment is constructed using Docker in a closed network environment that is not connected to the outside on a virtual guest OS. CyExec system build attack and defender practice environments on Docker container. Attacks that attack the vulnerability from the attacker to the defender are carried out, and communication contents regarding the attacker's attacks and the analysis of logs are carried out by the defense. Also, to develop the application part exercise requires high expertise and development time. By using CyExec, multiple higher education institutions and private companies can collaborate to develop an exercise program in the open community environment jointly [20]. Additionally, when training basic and applied exercises, CyExec will provide legal and ethical education contents to prevent the illegal use of attack technology by the intentions and misses of the learners.

The exercises adopt flip teaching, and the learners learn the relevant technology in advance by documents. Learners will participate in the exercises after learning the necessary skills.

5.2 Basic exercises(based on WebGoat)

In the basic exercises, learners learn about the outline of vulnerability, detection, and countermeasure. The exercise theme was selected in consideration of the high priority vulnerabilities shown in OWASP Top 10 and the curriculum corresponding to the higher education institutions [25]. The OWASP Top 10 is a result of the experts regularly update vulnerability detection and prevention methods for high-risk vulnerabilities, etc. Table 5 shows the correspondence between the CyExec theme and the OWASP Top 10. The selected exercise theme defines the learning level, and skills using the HMM and the SecBok introduced in Chapter 4.

Table 5: Correspondence between WebGoat and OWASP Top 10

No.	Category	Lesson Plan	OWASP Top 10
1	Introduction	Introduction	-
2	Basic knowledge	General	-
3	Vulnerability diagnosis	Injection Flaws	A1:2017-Injection
			A4:2017-XML External Entities (XML)
4		Athentication Flaws	A2:2017-Broken Authentication
5		Gross-Site Scription (XSS)	A7:2017-Cross-Site Scription (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 Comonents	A9:2017-Using Components with Known Vulnerabilities
11		Client side	-
12	CTF	Challenges	-

For example, a summary of the “SQL Injection” exercises is shown below.
(1) Purpose of the Exercises: The use of the basic exercises is to understand the basic knowledge of SQL, an outline of SQL injection and detection method, and to acquire necessary skills on cyberattack and defense through assignments.
(2) Capable Skills of Being Acquired: The following are examples of learnable skills. These items are selected from the SecBok skill table described in Chapter 4.

- 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 a code injection technique using a vulnerability that allows an application to execute unintended malicious SQL statements inserted into the 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 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 authentic, information that does not match the condition leaks.
(7) Assignments: Figure 3 shows an example of SQL Injection assignments.

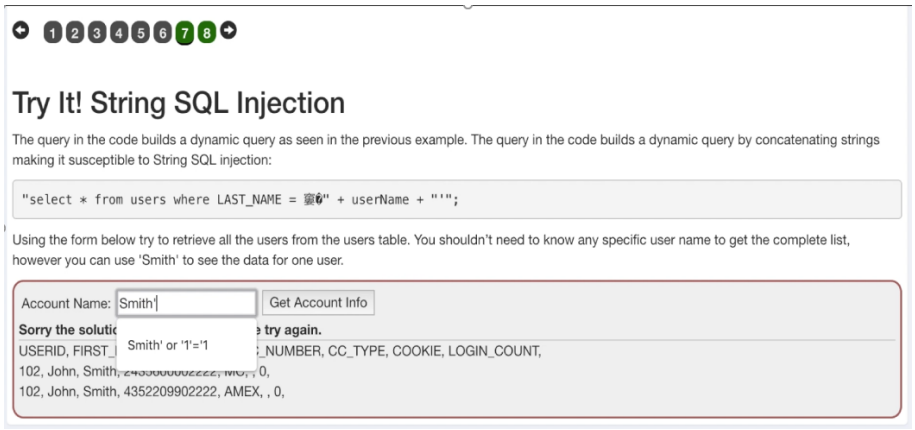

Figure 3: Example of assignments about string type SQL injection

5.3 Applied exercises (attack and defense)

After learning the basics of vulnerability measures in basic exercises, learners learn practical attack and defense techniques through the applied exercises. To respond to various attacks, assume actions from multiple viewpoints such as the attacking side, the defending side, the manager and the general user, and improve the ability to respond within the organization.

5.3.1 The Goal of the exercise

The goal of these exercises is to acquire cyber-attack and defense technology from the following viewpoints comprehensively. In the CyExec, attack technology is organized for learners can learn the defense technology genuinely.

- Understanding attack methods that exploit vulnerabilities: Vulnerability diagnosis using tools such as OWASP ZAP, and attacks that exploit software/server vulnerabilities
- Understanding defenses against attacks: Log detection and analysis of attacks, countermeasures against attacks

5.3.2 Skills that can be acquired

The following is an example of skills that can be learned. We selected the skills for exercise based on the SecBok skill table described in Chapter 4.

- Ability to identify systematic security issues based on vulnerabilities and system configuration information
- Knowledge of penetration testing principles, tools, and techniques
- Skills in performing vulnerability scans and vulnerability awareness in security systems
- Skills in using network analysis tools for vulnerability identification

5.3.3 Constitution of the exercise system

Figure 4 shows an overview of the exercise system configuration. The learners log in to the attacker or defender terminal running in the container on the CyExec and perform the exercise. Communication between terminals uses a virtual network set on a container. The attacker operates the terminal, try the unauthorized logins to the vulnerability of the defending web server via a virtual network, and prepares a script for the attack. The goal of the attacking side is to steal confidential information by attack script. Learners will carry out an exercise to monitor the communication contents from the attacking team and find out the information about the logs. Also, the defending side considers and implements measures against attacks such as unauthorized logins and then confirming that the attacks can be prevented.

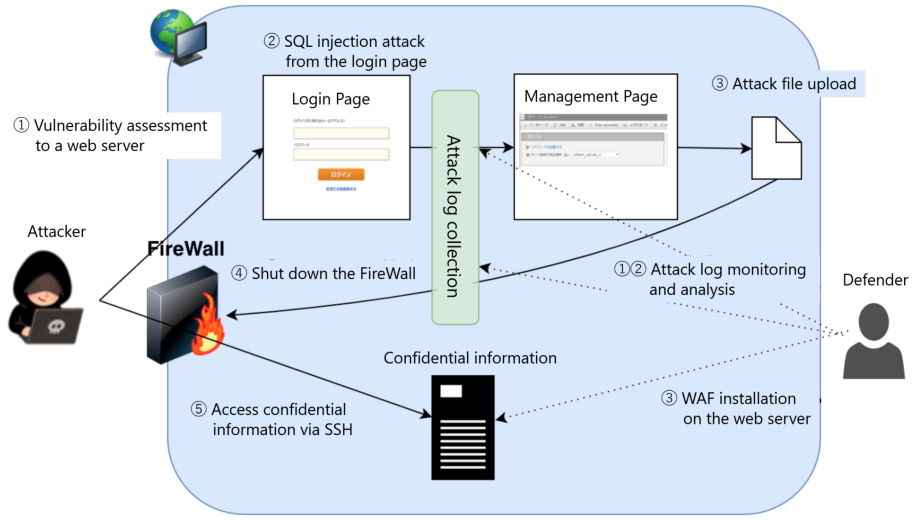

Figure 4: Constitution of the exercise system

5.3.4 *Exercise scenario*

Figure 5 shows the image of the attack scenario.

The following list is the content of the exercises on the attacker side.

1. Check the web server vulnerability using OWASP ZAP and write a report of the inspection result.
2. Execute a SQL injection attack to the web application which has a vulnerability and tries to unauthorized login.
3. Upload a script for the attack by using the file upload function of the screen after login
4. Access the attack script from the browser on the attacker side and execute the script. The attack script to stop the firewall.
5. Unauthorized access to the webserver using ssh command.

The following scenario is the content of the exercises by the defender side.

1. Monitor the log output at the time of attack using tools such as Apache Log Analyzer to detect the contents of attack script and SQL injection attack.
2. Edit the source code that has SQL injection vulnerability and confirms that it can prevent attacks.
3. Implement a WAF (Web Application Firewall) to verify that it can prevent unauthorized access to confidential information in the Web server.

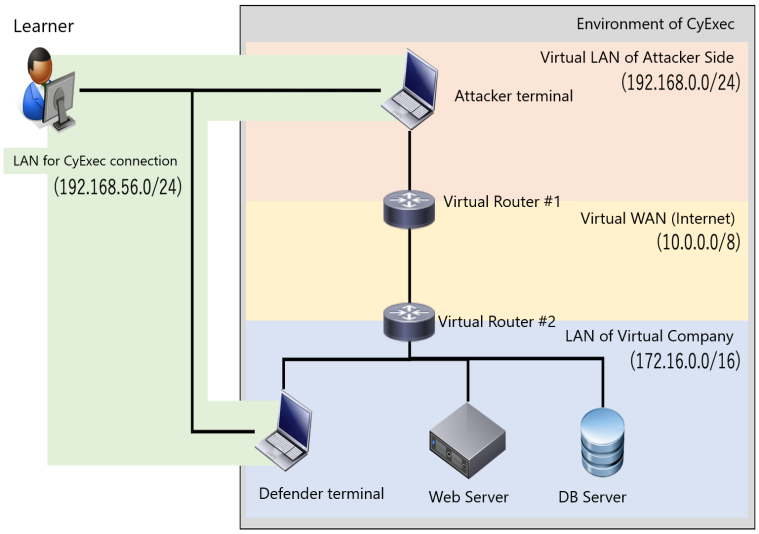

Figure 5: Image of exercise scenario

5.3.5 *Exercise example*

Figure 6 shows the system configuration of the applied exercise. We implemented Docker on a virtual environment configured with VirtualBox and installed a container on Docker. By implementing various exercise programs related to attack and defense, such as virtual digital signage and trap server used by attackers, and running them on containers, it is possible to construct an exercise environment for each purpose easily. We built a physical environment that imitated digital signage using Raspberry Pi. By connecting via CyExec, it is possible to perform safe exercises in an isolated environment from the outside while using the actual machine. By preparing IoT devices as a rial physical environment, the learner could imagine the actual situation of the attack. Therefore, we expect to enable easy-to-understand exercises with high educational effects. If a lecturer cannot prepare the physical environment, exercises in virtual environments only are also possible.

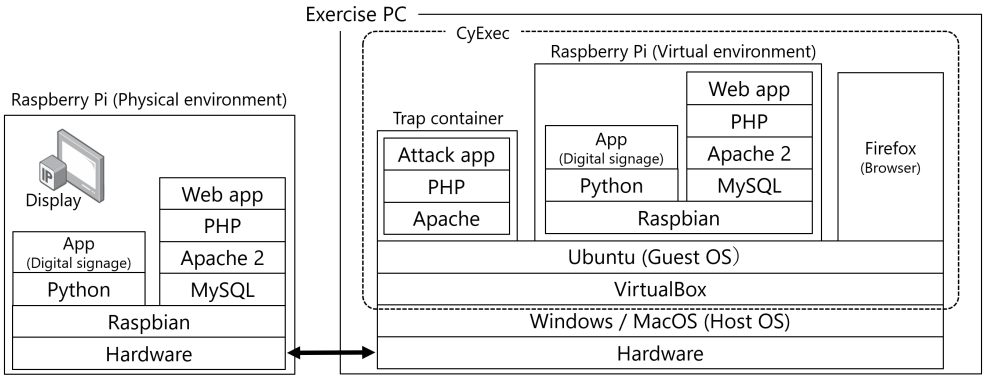

Figure 6: System configuration of the applied exercise

As an example of the applied exercise, we show the “Insecure Data Transfer and Storage.” This exercise is an exercise to eavesdrop unencrypted communication over HTTP or Telnet using the packet monitoring tool OWASP ZAP. This exercise corresponds to exercise “Access Control Flaws” and exercise “Insecure Communication” of WebGoat. An exercise “Access Control Flaws” of WebGoat learns about settings for which access control does not function correctly, and falsifies communication by using an OWASP ZAP. An exercise “Insecure Communication” learns about the HTTP encryption and intercepts authentication information included in communication by using the OWASP ZAP. Figure 7 shows an exercise to screen that the learner, in the CyExec exercise system uses OWASP ZAP to steal authentication information through network communication.

Figure 7: Example of applied exercises program

6 Conclusion

Cyber-attacks such as targeted attacks are increasing, and it is becoming a problem of digital society. Human resource development, which has attack and defense technology, is an important theme. Therefore, the environment improvement to security human resource development has not progressed due to the building cost of the exercise system and the shortage of personnel who maintain and manage the exercise environment. Therefore, we developed a cybersecurity exercise system CyExec, which is an ecosystem consisting of virtual computer environments using VirtualBox and Docker. The exercise content on the CyExec is a two-tiered structure, the basic exercise based on the WebGoat that OSS vulnerability diagnosis and learning program, and the applied exercise composed of attack and defense exercise. In this paper, we introduced the vulnerability diagnosis exercise using the WebGoat implemented in the CyExec, and the development of attack and defense exercise on the CyExec.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number JP 19K03006. This research carried out in the PBL (Project Based Learning) in the AIIT (Advanced Institute of Industrial Technology). In advancing the PBL, we got the cooperation of Ryo Watanabe, Katsumi

Komano, Shigeo Hatatani, Nobuaki Maki, Chen Sheng, and Daisuke Ishikawa. We would like to express our appreciation here.

References

[1] S. Shin et al., "Development of Training System and Practice Contents for Cybersecurity Education," Proc. 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), 2019, pp. 172–177.

[2] Information and Security White Paper 2019 (in Japanese), white paper, Information-technology Promotion Agency, Japan (IPA), Aug. 2019.

[3] National Center of Incident and Strategy for Cybersecurity, Japan, "Cybersecurity Strategy (in Japanese)," 7 Jul. 2018;
https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf.

[4] Ministry of Economy, Trade and Industry, Japan, "Survey on latest trends and future estimates of IT personnel (in Japanese)," Jun. 2016;
https://www.meti.go.jp/committee/kenkyukai/shoujo/daiyoji_sangyo_skill/pdf/001_s02_00.pdf.

[5] National Institute of Information and Communications Technology, "Practical cyber defense exercises Cyder (in Japanese)," Mar. 2019;
https://www.nict.go.jp/press/2019/03/20-1.html.

[6] K. Nakajima et al., "Proposal of an Environment for Practical System Security Learning From the Viewpoint of Hacker (in Japanese)," The 30th Annual Conference of Japan Society for Software Science and Technology, 2013.

[7] Ministray of Education, Culture, Sports, Science and Technology, Japan, "Annual report 2016," enPiT, 2017;
http://www.enpit.jp/img_new/publications/enPiT_annualreport_uni_2017.pdf.

[8] Cyber Defense Exercise with Recurrence; https://cyder.nict.go.jp/.

[9] A. Tomomi, "Effectiveness of Cyber Exercise - Toward Resilient Organization," Dec. 2015; https://www.jpcert.or.jp/present/2015/ICS20150212-NITech.pdf.

[10] N. Maki et al.,"An Effective Cybersecurity Exercises Platform CyExec and its Training Contents," International Journal of Information and Education Technology, vol. 10, no 3, 2020, pp. 215–221.

[11] OWASP Webgoat Project;
https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

[12] Information-technology Promotion Agency, Japan, 2018, "Vulnerability experience learning tool AppGoat," Jan. 2020; https://www.ipa.go.jp/security/vuln/appgoat/

[13] M. Sugawara et al., "Introduction of Attacker's Scenario to a Serious Game to Improve Capability of Cyber Security," Information Processing Society of Japan 79th National Congress, 2017.

[14] K. Nakashima, I. Kei and N. Ayahiko, “Proposal of An Environment for Practical System Se- curity Learning from the Viewpoint of “Hacker”,” The 30th Congress of the Japan Society of Software Science, 2013.

[15] M. Eture, “Practical Exercises for Cyber Attacks,” Information processing, vol. 55, no. 7, 2014, pp. 666-672.

[16] S. Yashiro et al.,“A Proposal and Implementation of Training System for Self-Studying targeted Attacks,” Information Processing Society of Japan 79th National Congress, 2017.

[17] S. Daisuke, “Implementation Planning of Penetration Testing Exercises for Raising Cybersecurity Awareness,” IECIE technical report, 2017.

[18] R. Beuran et al., “CyTrONE: An Integrated Cybersecurity Training Framework,” Proc. ICISSP, 2017, pp. 157-166.

[19] LAC Co., “Current Status and Trend of Information Security - Implementation procedure and practice examples of cyber exercises -,” 2015.

[20] T. Shinichi, etc., “Proposal of Cyber attack and defense Exercise system CyExec composed of ecosystem,” CSS2018, 2018.

[21] Releases WebGoat, Jan. 2019; https://github.com/WebGoat/WebGoat/releases.

[22] N. Ryotaro, H. Kumi and S. Yoichi, “Development of Container-based virtual exercise system CyExec related to cyber attack and defense,” The 80th National Convention of IPSJ, 2018.

[23] Japan Network Security Association, “SecBok Human Resources Skill Map (in Japanese),” 2017.

[24] OWASP Zed Attack Proxy Project Homepage;
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.

[25] OWASP Top Ten Project Homepage;
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.