Research Inventy: International Journal of Engineering And Science
Vol.13, Issue 7 (July 2023), PP 01-05
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Research, Design And Experiment A Multi-Platform Lab For Web Server Security Practice

Le Kim Trong
Vietnam Korea University of Information and Communications Technology – Danang University, Vietnam

Abstract:*Setting up a network lab in the teaching Networking and Information Systems Security can be very difficult because of hardware limitations and the complexity of managing a system of different servers. Students who want to gain a lot of hands-on experience need to practice on many different operating system platforms, but in current practice rooms, students are often exposed to only a few popular operating systems. To solve the above problem, in this article I have developed a practice system of web attack and defense techniques based on multi-platform technology with the help of DVWA and VMWare vSphere. Through the testing process, the implementation has brought many benefits in terms of practical teaching, increasing the quality of learning and research of students when participating in learning and practicing website attack and defense techniques, in addition, lecturers have more flexible management than before.*

Keywords:*Network and information system security, web application for attack practice, multi-web server system, virtualization technology, multi-platform labs,web server security.*

Date of Submission: 18-06-2023 Date of Acceptance: 02-07-2023

I. INTRODUCTION

In setting up an effective cyber security lab, it is generally necessary to provide the following: Make sure there are enough computers for students to practice; The computer should be powerful enough to run the necessary tools and software; A private network so students can perform network attacks and defenses on target servers; Tools like Wireshark, nMap, Metasploit, and network and server emulator platforms like VirtualBox or VMware; The target of the attack is the server and the target network with security vulnerability so that students can implement attack and defense techniques; Learning materials and resources including tutorials, references, and hands-on exercises to support student learning and research; Instructors and technical support: lecturers need to have knowledge of cybersecurity to guide and support students during practice, technical staff need to be ready to solve technical problems that students have may encounter.

In the practice of website attack and defense techniques, due to the limitations of hardware availability and budget constraints, there have been many limitations in the practice of students [9]. Students have little access to a variety of targets (security vulnerability). Practices often overlap as teams share the same target servers. To overcome this situation, there have been studies that use independent simulators to create a separate environment for groups of students, but these studies do not consider the process of cooperation between students and lack of comprehensive analysis of student learning behavior and learning outcomes.

In studies [2, 5, 6, 10, 13] they used virtualization to provide collaborative lab and shared resources. Studies [6, 8, 13] mentioned that collaboration between students in virtualized environments helped improve their knowledge and skills. However, the above studies currently only provide an alternative solution to the hardware problem and optimize costs by reducing the number of servers, not solving the main problem that students want to practice on multiple OS, a variety of server platforms and practice as many common types of security vulnerabilities as possible. Practicing diverse types of security vulnerabilities will help better shape the future network defense strategy [17]. Therefore, this study tried to find an effective solution for teaching website attack and defense practice in order to increase the amount of practice content and the number of platforms that students are accessible.

II. EXPERIMENTAL PROCEDURE

This study proposes a practice system of website attack and defense techniques based on VMWare vSphere virtualization technology and combines DVWA implementation and ManageEngine EventLog Analyzer to create a new practice environment for students. This system design study can reduce the workload of lecturer's practice room management thanks to the advantages that a virtualized-based system brings. At the same time, DVWA with a variety of the most common security vulnerabilities comes with a simple, intuitive and detailed operation mechanism that allows students to complete many exercises with less help from the lecturer.

1.1 System architecture proposal

- Network: Build a private intranet to create a safe and isolated environment for practice activities.

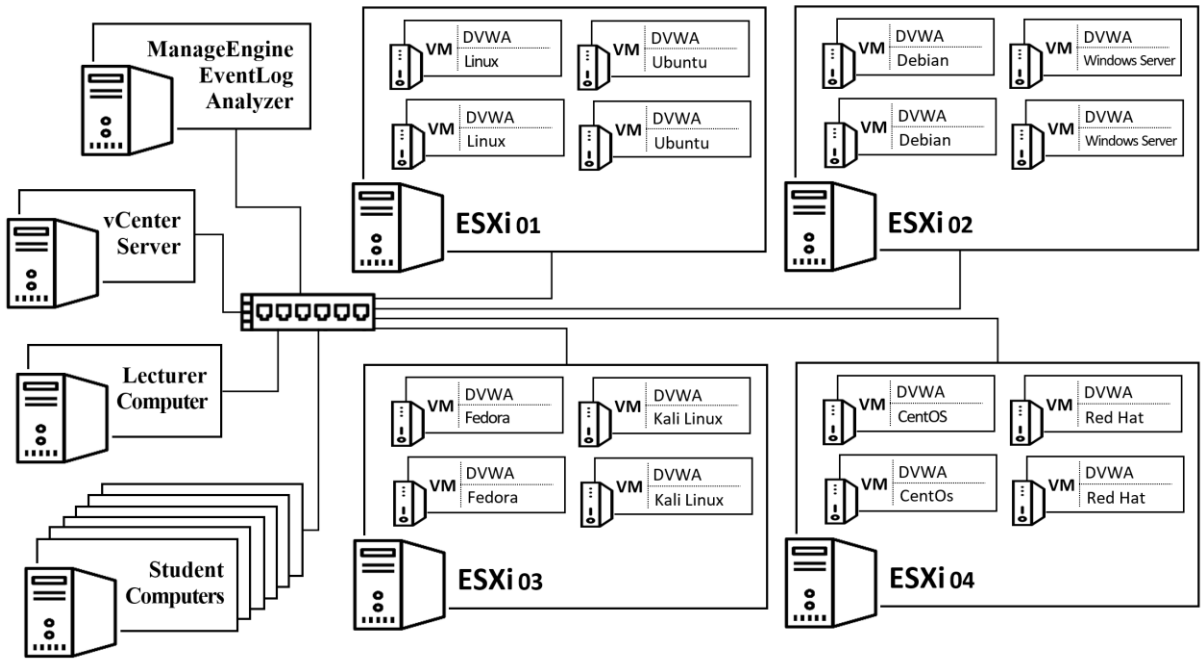
- Virtual Target Servers: Set up target servers with the most common security vulnerabilities by using DVWA. This allows students to perform website attacking techniques in a safe and legal environment.

- Management Server: Manage all virtual target servers, create new virtual target servers and allocate resources to them.

- Monitoring and Logging: Set up a monitoring and event recording system to monitor network activity and analyze attack behavior. Tools like ManageEngine EventLog Analyzer or Splunk can be used to collect and analyze log data.

In Figure 1, we can see the overall architecture of the system that this study proposes. DVWA (Damn Vulnerable Web Application) is a PHP/MySQL source code application that collects security logic errors. The main goal of DVWA is to create a legitimate base and advanced penetration testing or attack practice environment. DVWA is a free software application that can be redistributed or modified under the terms of the GNU general public license. DVWA fully meets the criteria as in the study [7] on the type of application suitable for website attack and defense practice.

Figure1. System Architecture Proposal



Research has built a model based on the VMWare vSphere platform that is able to evenly distribute system resources to all virtual machines and keep them in a tightly managed and monitored network. The practice room is designed with 16 virtual servers on 4 VMware ESXi servers, all managed by vCenter Server to ensure that they can operate stability and deliver the best performance during the student practice. At the same time, in case lecturers find that some virtual machines need more resources than usual, they can also specifically set the amount of system resources for those virtual machines, such as the amount of RAM, disk space, number of CPU cores, etc., quickly and easily.

1.2 Research methods

Description of the object

Four classes, each class includes 32 students, a total of 128 students studying the same module. The study time includes 22 theory periods and 16 practical periods, when students practice divided into 2 groups in 2 practice rooms:

+ Experiment Group abbreviated EG: consists of 64 students practicing in 2 practice rooms using the model as shown in Figure 1, 32 students in each room, divided into 16 groups, each small group of 2 students using 1 virtual machine target with a variety of operating systems.

+ Control Group abbreviated CG: consists of 64 students practicing in 2 traditional practice rooms, 32 students each, also divided into 16 groups, each small group of 2 students. Each room uses 4 physical servers, each physical server is a shared target for 4 small groups.

When practicing in each group, it is necessary to complete practical exercises related to the study attack and prevention of web server attacks such as: Brute Force, Command Execution, Cross Site Request Forgery (CSRF), File Inclusion, SQL Injection, Insecure File Upload, Cross Site Scripting (XSS), etc., based on the goals that the lecturer assigns to each group.

Dependent variables

Dependent variables include: time to prepare the practice room of the lecturer before the practice sessions of the 2 groups, the test scores before and after the practice process, and the combined practice test scores.

Research tools

The practice rooms use the model in Figure 1; Tests before and after the practice process; combined practice test . The content of the test before the practice process includes the basic theories learned in the theory part, the content of the test after the practice process includes advanced theories, questions to assess the depth of understanding and application of key issues of the course. The combined practice test tests the most important parts of the course from the beginning of the semester to the end of the semester.

Monitoring issues and statistical tools

The study used the IBM SPSS Statistics 25 statistical software to make statistics and analyze the data collected from the experiment. The main purpose is to analyze the results of the activities, the results of the tests clearly and objectively, to determine whether there is a statistically significant difference in the collected data.

EG team lab monitoring: can be performed continuously and live at any time through monitoring from vCenter server and ManageEngine EventLog Analyzer server based on log data analysis. In contrast, the supervision in the practice room of the CG group is conducted after the students have finished practicing or at the end of the lesson, because the supervision on the real server is limited when the students are practicing the target directly on the server, monitoring parameters can disrupt the practice portion of student groups.

III. RESULTS AND DISCUSSIONS

3.1 T-test results of pre-test

The purpose of testing the basic knowledge learned in theory before participating in practice (pre-test) is to ensure that both groups of CG and EG students have the same basic knowledge before participating. In Table 1, the Sig of F test equals 0.610 > 0.05 ie there is no difference in variance between the two groups, CG and EG, we will use the t test results in the row Equal variances assumed. the Sig of t is equal to 0.799> 0.05 and in Table 2, the pre-test statistical results show that there is no significant difference between the CG control group with the mean score value of 6.159 and the EG experimental group with the mean score value of 6,084. In summary, the hypothesis can be accepted that there is no difference between the CG and EG groups, that is, there is no common difference in basic knowledge between the two groups before participating in the practice process.

Table 1. Independent samples test results ofpre-test.

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Theory test (Pre-test)	Equal variances assumed	.262	.610	.256	126	.799	.0750	.2932	-.5052	.6552
	Equal variances not assumed			.256	125.527	.799	.0750	.2932	-.5052	.6552

Table 2. Group statistic results of pre-test.

Group Statistics					
	Group	N	Mean	Std. Deviation	Std. Error Mean
Theory test (Pre-test)	CG	64	6.159	1.7087	.2136
	EG	64	6.084	1.6069	.2009

3.2 T-test results of post-test

Next, the purpose of the advanced extended theory test after participating in the practice (post-test) is to test whether two groups of students CG and EG after the practice process, acquire more extended knowledge from is the practice equivalent? In Table 3, the Sig of F is equal to 0.682 > 0.05, that is, there is no difference in variance between the two groups CG and EG, we will use the t-test results in the row equal variances assumed. Sig of t equals 0.000 < 0.05 and in Table 4, the results show that there is a significant difference between the CG control group with a mean score of 5.631 and the EG test group with a better mean score of 7.017. In summary, it can be concluded that there is a statistically significant difference in this case. That is, the group of EG students gained more knowledge through practice than the group that practiced in the traditional lab. This can be explained by the number of vulnerabilities and the rich number of operating systems and the superiority of the virtualization system, which helps the practice on the platform to be more independent, with more supporting features such as: Easy backup, restore, and customization of hardware parameters have had a positive impact on student practice.

Table 3. Independent samples test results ofpost-test.

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Theory Test (Post-Test)	Equal variances assumed	.169	.682	-5.609	126	.000	-1.3859	.2471	-1.8749	-.8970
	Equal variances not assumed			-5.609	126.000	.000	-1.3859	.2471	-1.8749	-.8970

Table 4. Group statistic results of post-test.

Group Statistics					
	Group	N	Mean	Std. Deviation	Std. Error Mean
Theory Test (Post-Test)	CG	64	5.631	1.3985	.1748
	EG	64	7.017	1.3970	.1746

3.3 T-test results of combined practice test

The organization of a combined practice test is to check whether there is a difference after the practice of two groups of CG and EG students in their ability to practice web server attack and defense techniques. In Table 5, we see that the Sig of F test is equal to 0.260 > 0.05, so there is no difference in variance between the two groups CG and EG, we will use the results of the t test in the row Equal variances assumed. Here, Sig of t equals 0.000 < 0.05 and in Table 6, the results show that there is a significant difference between the CG group with the mean score of 6.09 and the EG group with a better mean score of 7.72. In summary, with the above data, it can be concluded that there is a statistically significant difference in this case. That is, after completing the hands-on learning process, the EG group of students has better practice ability than the practice group in the traditional lab.

Table 5. Independent samples test results ofcombined practice test.

Independent Samples Test									
	Levene's Test for Equality of Variances		t-test for Equality of Means						
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
								Lower	Upper

Combined practice test	Equal variances assumed	1.283	.260	-7.047	126	.000	-1.625	.231	-2.081	-1.169
	Equal variances not assumed			-7.047	122.450	.000	-1.625	.231	-2.081	-1.169

Table 6. Group statistic results of combined practice test.

Group Statistics					
	Group	N	Mean	Std. Deviation	Std. Error Mean
Combined practice test	CG	64	6.09	1.411	.176
	EG	64	7.72	1.188	.149

In addition, during the practice process, the time to prepare the practice room of the EG group, the lecturer always has a great advantage in the preparation process and shortens the time to prepare the lab room before students begin to participate in practice.

IV. CONCLUSION

This study demonstrates the effectiveness of multi-platform labs on web server security practice, where students can enhance their practice on web server attack and defense with a wider variety of different platforms that virtualization offers. VCenter and ManageEngine EventLog Analyzer allows lecturers to manage student's practice activities and capture the status of virtual servers quickly. Virtualization and network emulation tools as core technologies allow teachers to create multiple virtualized network topologies and change virtual server hardware flexibly to respond well to the needs that arise in the student's practice process . Accordingly, the students had a more complete practice process and did not face many problems of conflicting goals with other groups. Features such as backing up the server state so that they can be restored at any time give students confidence in their practice and don't spend a lot of time troubleshooting problems or manipulation errors during practice. The results of the tests may indicate that the students in the Experiment Group benefited from the new laboratory model. In addition, the lecturers also benefited greatly in the preparation of the machine room and in the process of monitoring and recording student performance.

REFERENCES

[1]. A.Konak, M. Bartolacci, 2012. Broadening E-commerce information security education using virtual computing technologies. Networking and Electronic Commerce Research Conference.

[2]. A.Zenebe, D. Anyiwo, 2010. Virtual Lab for Information Assurance Education. 14th Colloquium for Information Systems Security Education, Baltimore Marriott Inner Harbor.

[3]. B.Hay, K. Nance, C. Hecker, 2006. Evolution of the ASSERT Computer Security Lab. 10th Colloquium for Information Systems Security Education, Adelphi, MD.

[4]. D.Davis, 2006. Top resources to learn about vCloud director - VMware vCloud Blog. VMware vCloud Blog.

[5]. J. Keller, R. Naues, 2006. A Collaborative Virtual Computer Security Lab. E-Science and Grid Computing.

[6]. J. M. Jones, K. K. Augustus, P. Li, 2011. Incorporating virtual lab automation systems. American Society for Engineering Education, vol. 22, no. 856, 1-13.

[7]. J. M. Porup, 2018. Learn to play defense by hacking these broken web apps. CSO Online.

[8]. J. Son, C. Irrechukwu, P. Fitzgibbons, 2012. A Comparison of Virtual Lab Solutions for Online Cyber Security Education. Communications of the IIMA, vol. 12, no. 4.

[9]. K. Nance, B. Hay, R. Dodge, J. Wrubel, S. Bird, A. Seazzu, 2009. Replicating and Sharing Computer Security Laboratory Environments. The HICSS Conference.

[10]. M. Aboutabl, 2006. The cyberdefense laboratory: A framework for information security education. Information Assurance Workshop.

[11]. M. E. Whitman, H. J. Mattord, 2004. Designing and teaching information security curriculum. 1st annual conference on Information security curriculum development, New York.

[12]. M. Whiteman, H. Mattford, 2009. Risk Management. Principles Of Information Security, Course Technology, p. 11.

[13]. P. Li, L. W. Toderick, P. J. Lunsford, 2009. Experiencing virtual computing lab in information technology education. ACM conference on SIG- Educational Information Security Laboratories.

[14]. R. Dodge, R. C., C. Bertram, D. Ragsdale, 2007. Remote Virtual Information Assurance Network. IFIP International Information Security Conference, Springer US.

[15]. V. Anantapadmanabhan, Nasir Memon, P. Frank, Gleb, 2003. Design Of A Laboratory For Information Security Education. IFIP-The International Federation for Information Processing, vol. 15, 61-73.

[16]. V. Padman, N. Memon, 2002. Design of A Virtual Laboratory for Information Assurance Education and Research.the 2002 IEEE Workshop on Information Assurance and Security , West Point, NY.

[17]. Yuri Diogenes, Erdal Ozkaya, 2019. Cybersecurity - Attack and Defense Strategies. Packt Publishing.