# VILARITY - Virtual Laboratory for Information Security Practices

Irfan Syamsuddin

*Center for Applied ICT Research, Computer and Networking Engineering, Politeknik Negeri Ujung Pandang, Makassar, Indonesia*

***Abstract*** **– Availability of teaching aid for laboratory practices is important particularly in the field of information security. In this paper is introduced a novel Virtual Lab for Information Security practices called VILARITY. It is an on-going effort to establish alternative laboratory based on virtualization technology specifically designed for two security related courses. The paper at hand briefly presents assessment for VILARITY usage through two different surveys. The first survey aims to assess the effectiveness of contents of Virtual Lab whilst the second one is to find out any obstacles faced by students in using virtualization tool. In conclusion, most students consider hands on practices with the Virtual Lab have enhanced their skills and knowledge and the virtualization environment is appropriate for delivering the practices.**

***Keywords*** **– Virtual lab, information security, virtualization, laboratory practices, evaluation.**

## 1. Introduction

Computer networks have been increasingly popular along with ever more reliance of people to information technology in daily life. The proliferation of computer network in all disciplines and work area such as government, education and business institutions has created huge demand for skillful IT staff with computer network experiences.

On the other hand, while more concerns towards the importance of reliable computer networks have been gathering pace, few of them start to realize the dark side of computer networks misuse that could bring the organization into serious problems.

In recent years many organizations have been seeking IT staff being not only able to maintain network management and administrative tasks but also having security related skills and knowledge. Therefore, higher educational institutions need to response these trends by providing students with the required courses in security.

To tackle the issue of producing skilled human resources in the area, at the State Polytechnic of Ujung Pandang, Indonesia, students majoring Computer & Network Engineering are offered two security related courses as determined in the curriculum, namely Computer Network Security and Information Security Management as suggested by the current curriculum [1],[2]. Both courses consist of a number of hands on laboratory practices designed according to the theoretical topics discussed.

However, establishing ideal computer lab with sophisticated hardware for network security exercises usually requires very expensive cost [3] which is mainly difficult for the campus to fulfill. As a result, the lecturer should find alternative to keep students able to perform hands on practices. A novel approach was introduced by exploiting virtualization technology to develop VILARITY (Virtual Laboratory for Information Security)[4]. The virtual lab is based on Linux operating systems with several network simulators' software combined within. Early version of the Virtual Lab is actually for general purposes (for all networking courses lab requirements), however in this case it is used specifically for the two aforementioned security courses.

This paper aims to assess the usability of VILARITY in helping students to perform security related hands on practices as determined by the two courses. The paper is structured into 5 sections. Section 2 describes literature review, while the

DOI: 10.18421/TEM83-45
https://dx.doi.org/10.18421/TEM83-45

**Corresponding author:** Irfan Syamsuddin,
*Center for Applied ICT Research, Computer and Networking Engineering, Politeknik Negeri Ujung Pandang, Makassar, Indonesia*
**Email:** *irfans@poliupg.ac.id*

*Received: 31 March 2019.*
*Revised: 14 July 2019.*
*Accepted: 17 July 2019.*
*Published: 28 August 2019.*

methodology and tools used to conduct the research are presented in section 3. Then, the results and the discussion are given in section 4. Finally, the study is summarized in the last section.

## 2. Literature Review

Virtualization is an advanced technology that enables operating systems (OS) running over other operating systems without the need to make logical hard drive partition like previously [5]. Besides, virtualization technology enables a computer to run multiple virtual machines simultaneously, while each virtual machine running a different and isolated operating system [6].

The building block of virtual machine technology is presented in Figure 1. [3]. A Virtual Machine Monitor (VMM) is typical application similar to other applications running over the main or host operating systems in a personal computer. However, over a VMM, one may create a Virtual Machine that runs one guest operating system. Then, any applications might be installed and operated over the guest OS [7],[8].

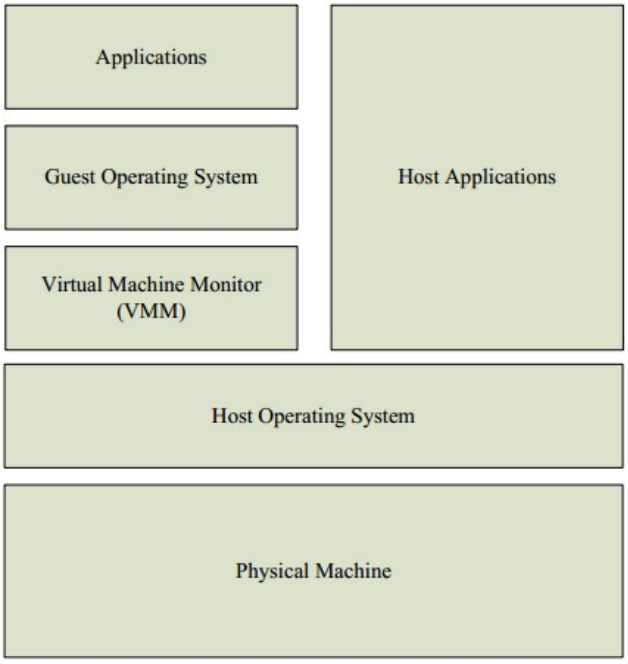


*Figure 1. Building block of virtualization technology*

Its flexibility makes virtualization widely applied in developing virtual laboratory. Willems and Meinel [8] introduce Tele-Lab which is aimed at supporting remote training based on virtual environment. A large scale virtualization initiative was described in study by Soceanu, at.al [9]. They developed virtual labs and applied them to support online EU courses incorporating open source technologies.

Benefits and advantages of using virtualization in the educational sector were also emphasized in a study by Miseviciene et al. [10]. They highlight the importance of infrastructure advancements and other educational functions to make learning resources virtually available anywhere and at any time. In addition, employing virtualization to educational ICT infrastructure provides a flexible and cost-effective platform in case a single server may operate several operating systems and sharing computing resources [11].

## 3. Methodology and Tools

Based on advantages offered by virtualization technology, an initial effort to create a new virtual lab environment to support hands on exercises of several computer networks courses at the Department of Computer and Networking Engineering of State Polytechnic of Ujung Pandang is described in [3]. To extend that work, here we present VILARITY, a novel Virtual Laboratory for Information Security course. It is also based on Virtual Box as VMM, mainly due to open source considerations [12].

Following the previous study, the development of virtual lab was also based on ADDIE model. Advantages of using ADDIE model are mainly due to its well-structured and straightforward approach formulated in the five stages approach [13]. Figure 2. shows five stages of ADDIE model namely design, development, implementation and evaluation.

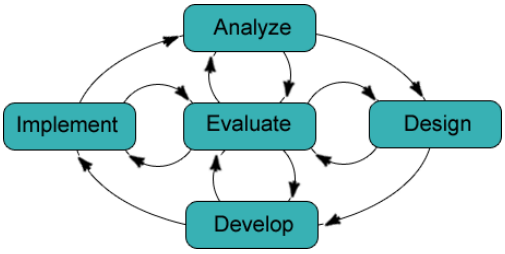


*Figure 2. ADDIE Model*

Our preliminary study [3] describes all steps in developing the Virtual Lab in accordance to the five stages of the ADDIE Model. Within the Virtual Lab, several open source simulation softwares are combined and specifically used in this case to support hands on practices of two security related courses.

VILARITY Virtual Lab as depicted in Figure 3. consists of the following laboratory activities:

### a. Basic Virtual Machines

In this topic, students are assisted to perform several hands on practices such as VirtualBox installation and management, deploying VILARITY as Virtual Machine and testing VM performance. This topic requires 3 weeks to finish.

### b. Advanced Terminal Commands

In this topic, which requires 4 weeks for a student to finish it, there are several activities such as testing VirtualBox Host-Only Networks, introduction to perform footprinting technique, practical FP using nMAP tool, and DNS information collection

### c. MITM Man In The Middle Attack Lab

This topic covers several activities, such as setting Web Server, FTP Server, capturing passwords on live network, capturing files transmitted on network and packet data view. It is expected to take 4 weeks to finalize this topic.

### d. Web Hacking Exercise

In the last section that requires 5 weeks including report, student sets up a web server to operate Content Management Systems, perform footprinting on the CMS, attack the CMS using SQL injection technique and finally conduct a brute force attack on CMS.

In general, to finalize all courses' contents, it requires 14 live hands on practices with four experiment reports.

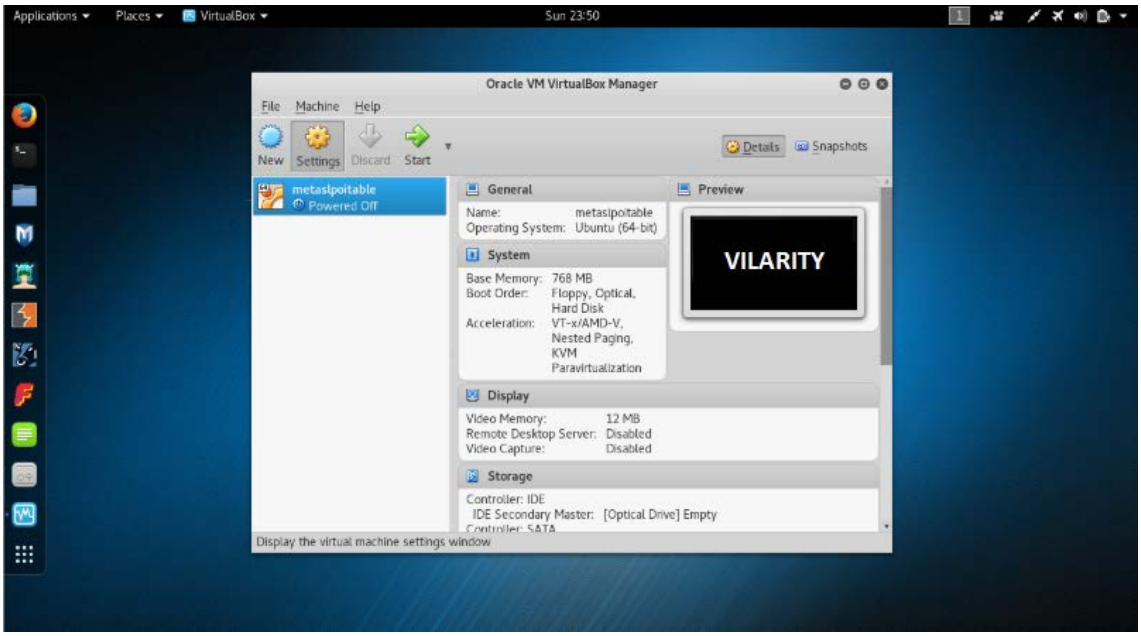


*Figure 3.. VILARITY Virtual Lab*

*Table 1. Survey of Virtual Lab for security hands on practices*

| *Survey Questions* | *SD* | *D* | *N* | *A* | *SA* |
|---|---|---|---|---|---|
| Q1. Effectiveness of exercises in the virtual lab are as good as those in ones in a physical computer lab | 0 | 2 | 2 | 18 | 24 |
| Q2. Virtual lab is useful for self-study | 0 | 5 | 2 | 21 | 18 |
| Q3. Students are able to obtain security related skills and knowledge with virtual lab | 0 | 1 | 2 | 22 | 21 |
| Q4. The lab instruction in job sheets are clear and easy to understand | 0 | 1 | 8 | 21 | 16 |
| Q5. The lab exercises are well organized | 0 | 1 | 5 | 15 | 25 |
| Q6. The topic of each exercise is related to security theory in lectures | 0 | 0 | 3 | 26 | 17 |
| Q7. The topic of each exercise is helpful to understand topics in lectures | 0 | 0 | 3 | 15 | 28 |

Presently, we have reached the last stage of ADDIE Model (evaluation stage), therefore the focus of current study is to perform evaluation on the use of Virtual Lab for Computer Network Security and Information Security Management courses.

Following the implementation of VILARITY, two surveys are created according to previous study by Li, et.al.[14]. The first survey aims to assess student perception regarding content and effectiveness of the Virtual Lab in supporting the courses, while the purpose of the second one is to identify obstacles experienced by students in using virtualization technology (in this case Virtual Box) to run the Virtual Lab.

## 4. Results and Discussion

The first survey consists of seven questions covering all aspects of Virtual Lab for security hands on practices from student perspective. The results are presented in Table 1.

In terms of the first question, students are pleased with the overall effectiveness of the virtual lab; majority of them agree (18 students) or strongly agree (24 students), while few of them selected neutral, and disagree (4 students). Then, in the second question it is revealed that most students agree (21 students) or strongly agree (18 students) that the virtual lab is useful for them for self-study.

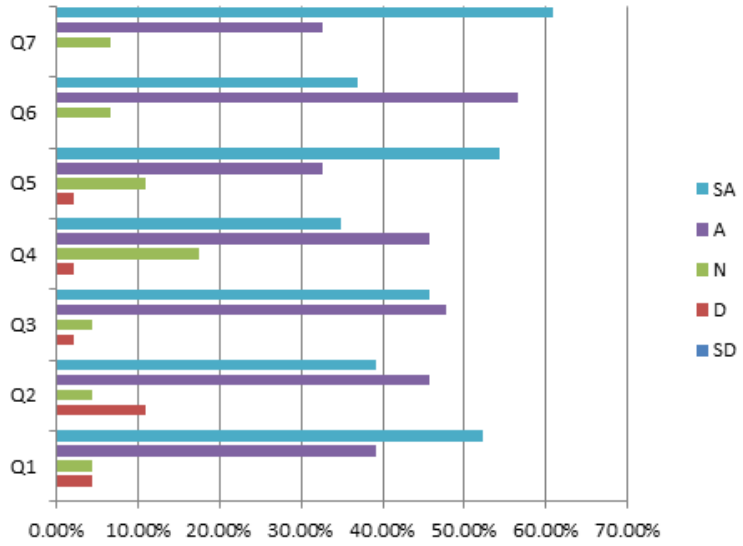


*Figure 4. Survey result in percentage format.*

*Table 2. Second survey on obstacles in using Virtual Box*

| *Do you have any problems using Virtual Box ?* |
|---|
| A1. Virtual Box is difficult to install and operate |
| A2. Virtual Box is time consuming |
| A3. Virtual Box makes computer slower |
| A4. Virtual Box consumes many resources of the computer |
| A5. Difficult to run security simulations over Virtual Box |
| A6. Other issues |
| A7. No problem at all |

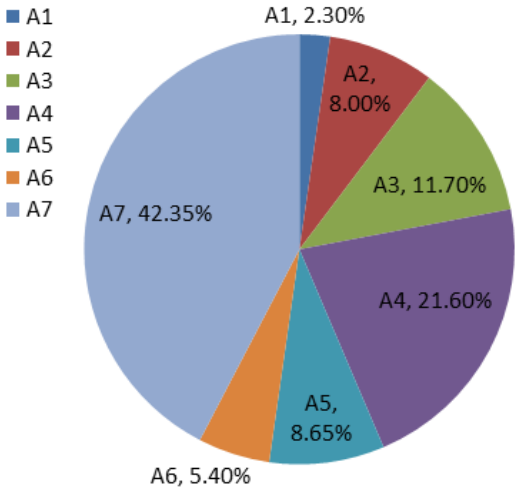


*Figure 5. Result of the second survey*

Only 5 students disagree and other 2 students are neutral in this regard.

In the third question, 43 students acknowledged that their skills and knowledge are improved using the virtual lab, while only 2 students selected neutral and another student disagreed. For the fourth question, it is found that the lab instruction provided along with the virtual lab is sufficient enough for students' needs as seen that 21 students agreed and 16 others strongly agreed whilst 8 students selected neutral and one of them disagreed. Then, in the next question, similar pattern is found that the majority of the students agreed and strongly agreed of 40 students in total, the rest are neutral (5 students) and only one of them disagreed.

The last two questions also present similar results as follows. For the sixth question, 43 out of total 46 students agree and strongly agree that each exercise is in line with theory in face to face meeting in class. Only three students chose neutral option in this regard. Similarly, students had no doubt regarding their understanding obtained in relation to each exercise, majority of them agree (15 students) or strongly agree (28 students) while neutral option was selected by only 3 students. Overall, it is clearly seen that high percentage of students consider the Virtual Lab as beneficial in enhancing their skills and knowledge in both security related courses (see Figure 4.).

The second survey is aimed at identifying obstacles faced by students in using virtualization technology. The survey is simply a question with seven optional answers; each represents specific issue of virtualization by which students possibly feel it uncomfortable during the lab exercises (Table 2.).

The survey structure is made by following approach in [14] and [15] with some modifications according to this study. Each student may only choose one of seven available answers according to the experience they faced in using Virtual Box.

The results are depicted in Figure 5. It is found that only 2% of students feel it hard to work over Virtual Box as the environment of our Virtual Lab. Some students (8%) require more time since they have no prior experience with Linux operating systems. In the third question, many students (approximately 11.7%) report that their computer runs slower when running the Virtual Lab. In line with this, in question 4 approximately 26.6% of students found Virtual Box used too many resources (CPU, Memory, Space, etc.). As a result, it is reasonable to see that around 8.65% of students are facing difficulties in running their simulations over Virtual Box. While other unclassified issues are chosen by 5.4% of students, majority of students (approximately 37.35%) do not have problems in this case. Overall, it can be concluded that the selection of Virtual Box is considered appropriate by the students in running the Virtual Lab.

Although students generally stated VILARITY was very interesting to use and very helpful for them in improving their understanding of courses, there were several complaints expressed in the second survey. Among the problems that students complain about are the limitations of PC memory used to run a Virtual Machine. This results in a slow lab process that always consumes full memory while operating. Another problem by a number of students is the limited time of the second practicum which is an obstacle in the hands on practice.

Based on the findings, future research will be directed to improvements on VM to reduce barriers in using virtualization technology. For instance, repackaging current Virtual Lab to control memory allocations [16], or using approach in [17] to reduce the total CPU energy consumption.

## 5. Conclusion

This study presents an on-going research of VILARITY (Virtual Laboratory for Information Security Practices), in terms of its usage in supporting the hands on practices of two security related courses, namely Computer Network Security and Information Security Management. Two surveys delivered to students with two distinct objectives.

In the first survey which is intended to assess student perception regarding content and effectiveness of the Virtual Lab in supporting both courses, students strongly appreciate it and consider it as beneficial to enhance their skills and knowledge.

In the second survey regarding obstacles in using virtualization technology, it is revealed that highest percentage of students (42.35%) reported that they have no problems at all, while some of them complain on exhaustion of computer resources (21.6%), their computer became slower (11.7%) and other obstacles in total of 24.35%.

The findings from both surveys suggest that the use of Virtual Lab is useful and benefit students' skills and knowledge in both courses and most students are able to conduct hands on practices through virtualization technology. Future works will be directed to overcome current obstacles in order to improve the efficiency of our Virtual Lab in the near future.

**Acknowledgements**

*The author would like to thank Ministry of Research and Higher Education, Indonesia for financial support and to member of CAIR PNUP for supporting the study.*

**References**

[1]. Harris, J., & Jovanovic, V. (2018). Standards Driven Curriculum for Secure Software Development. *Issues in Information Systems*, *19*(3), 131-138.

[2]. Kim, H., Han, Y., Kim, S., & Choi, M. (2005). A curriculum design for e-commerce security. *Journal of Information Systems Education*, *16*(1), 55-64.

[3]. Kizza, J. M. (2009). *Guide to computer network security* (p. 341). London: Springer.

[4]. Syamsuddin, I. (2017, September). A Virtual Lab Model to Integrate Computer Networking Courses. In *2nd International Conference on Education, Science, and Technology (ICEST 2017)*. Atlantis Press.

[5]. Sahoo, J., Mohapatra, S., & Lath, R. (2010, April). Virtualization: A survey on concepts, taxonomy and associated security issues. In *2010 Second International Conference on Computer and Network Technology* (pp. 222-226). IEEE.

[6]. Semnanian, A. A., Pham, J., Englert, B., & Wu, X. (2011, April). Virtualization technology and its impact on computer hardware architecture. In *2011 Eighth International Conference on Information Technology: New Generations* (pp. 719-724). IEEE.

[7]. Li, Y., Li, W., & Jiang, C. (2010, July). A survey of virtual machine system: Current technology and future trends. In *2010 Third International Symposium on Electronic Commerce and Security*(pp. 332-336). IEEE.

[8]. Willems, C., & Meinel, C. (2011). Practical network security teaching in an online virtual laboratory. In *Proceedings of the International Conference on Security and Management (SAM)*(p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[9]. Soceanu, A., Vasylenko, M., & Gradinaru, A. (2017). Improving cybersecurity skills using network security virtual labs. In *Proceedings of the International MultiConference of Engineers and Computer Scientists 2017 Vol II, IMECS*.

[10]. Miseviciene, R., Ambraziene, D., Tuminauskas, R., & Pažereckas, N. (2012). Educational Infrastructure Using Virtualization Technologies: Experience at Kaunas University of Technology. *Informatics in Education*, *11*(2), 227-240.

[11]. Son, J., Irrechukwu, C., & Fitzgibbons, P. (2012). Virtual lab for online cyber security education. *Communications of the IIMA*, *12*(4), 5.

[12]. Li, P. (2010). Selecting and using virtualization solutions: our experiences with VMware and VirtualBox. *Journal of Computing Sciences in Colleges*, *25*(3), 11-17.

[13]. Allen, W. C. (2006). Overview and evolution of the ADDIE training system. *Advances in Developing Human Resources*, *8*(4), 430-441.

[14]. Li, P., Mohammed, T., Toderick, L., Lunsford, P., & Li, C. (2008, June). A portable virtual networking lab for IT security instruction. In *Proceedings of 2008 ASEE Annual Conference*.

[15]. Syamsuddin, I. (2018). Evaluation of NgeXTEA-a cryptography learning module. *Global Journal of Engineering Education*, *20*(3), 196-200.

[16]. Xiao, Z., Song, W., & Chen, Q. (2012). Dynamic resource allocation using virtual machines for cloud computing environment. *IEEE transactions on parallel and distributed systems*, *24*(6), 1107-1117.

[17]. Sharma, P., Chaufournier, L., Shenoy, P., & Tay, Y. C. (2016, November). Containers and virtual machines at scale: A comparative study. In *Proceedings of the 17th International Middleware Conference* (p. 1). ACM.