Collaborative Learning in Virtual Computer Laboratory Exercises

Ryan Richards, Abdullah Konak, Michael R. Bartolacci, and Mahdi Nasereddin
Penn State Berks

Abstract

Information security is becoming an important concern for many organizations. However, it is difficult to provide adequate amounts of hands-on learning opportunities for information security students due to campus information security policies, the high cost of specialized computer laboratories, and a lack of beneficial laboratory activities that satisfy students' educational needs. At Penn State University-Berks, we developed a collaborative virtual computer laboratory (CVCLAB) which hosts a collection of virtual machines on which students can test their skills without affecting physical computers in Penn State's physical network. Students are granted full administrative privileges on the virtual machines and can perform high risk operations that are not usually allowed on the campus computers and networks. In the last three years, we have investigated the utilization of virtual machines for teaching information security skills in both group and individual settings. In this paper, we discuss the impact of collaborative activities performed in the CVCLAB on student learning based on our empirical studies. We conducted a series of experiments in the CVCLAB environment where two groups of students completed two different versions of the same activity: group work and individual work. After the activity was completed, students were asked to complete a survey that evaluated their perceived learning and overall experience. The results showed that collaborative learning had a significant positive impact on student learning experiences.

I. Introduction

As is the case in many technical fields, hands-on learning is very important in an information security context. Information security students are expected to have not only a theoretical understanding of information security concepts, but also practical skills to identify security threats, implement security mechanisms to defend against them, and restore compromised information systems. Such practical skills can only be gained through hands-on experimentation. In the literature, ethical hacking[1, 2] involving "red team/blue team" activities[3-5], are recommended for teaching advanced skills to information security students. More importantly, hands-on experimentation is an effective pedagogy to teach students higher order thinking skills as defined within Bloom's taxonomy, including analysis, evaluation, synthesis and creation. A well designed hands-on activity can integrate skills from multiple levels of the taxonomy, thereby enhancing students' technical, as well as critical, thinking skills.

Providing information security students with hands-on experimentation is challenging. Many educational institutions have stringent IT policies that restrict student privileges on campus computers, thus limiting their ability to perform any meaningful information security tasks. Advanced information security activities such as hacking and blue/red team activities require

specialized computer laboratories that are usually isolated from the campus network infrastructure in order to prevent malicious activities. However, these specialized computer laboratories are expensive to establish and difficult to maintain. In addition, students do not have the opportunity to practice their skills outside of regular laboratory sessions because of limited access. In the last decade, virtual computer laboratories have been replacing physical specialized computer laboratories and allowing for more flexibility for students and instructors. Table 1 summarizes a list of the VCL cited in the information security literature.

Table 1. A list of VCL for Information Security (VCL is used if no name is specified)

Laboratory/ Reference	**Area**	**Focus**	**Platform**	**Experimentation with Users**	**Pedagogical Evaluation**	**Remote Access**
Open Virtual Lab[6]	Computer Networking	Technical Design	Open Source	2 Case studies	None	Yes
V-Lab[7]	Network Security	Technical Design	Xen Server and OpenStack	None	None	Yes
VCL[8]	Computer Science	Technical Design	VMWare/VirtualPC	None	None	No
VCL [9]	Network, Security and Database	Technical Design	VMWare	The way 3 courses uses the system was presented	None	No
VCL[10]	Networking, Development, and Database	Technical Design	Windows	None	None	Yes
SWEET[11]	Cryptography	Technical Design	Virtual PC	28 students evaluated the system	None	No
VCL [12]	Information Systems	Technical Design	Redhat and Xen	None	None	Yes
Integrated Virtual Environment[13]	Theory of Computation (Finite state machine)	Technical and Pedagogical	Web	Four studies evaluates learning preferences of students (motivation, performance, and feedback)	Yes	Yes
Tele Lab[14]	Network Security	Technical Design	VNC	None	None	Yes
Velnet[15]	Computer Networking	Technical Design	VMWare	None	None	Yes
CenLavi[16]	Computer Networking	Technical Design	Open Source, Cloud	prototype was used	None	Yes
Virtual Lab[17]	Network Security	Technical Design	VMWare	None	None	Yes
The Collaboratory[18]	Computer Science and Engineering	Technical Design	Open Source	None	None	Yes

In addition to their technological and financial advantages, VCLs also promise new opportunities for enhancing student learning through collaborative and inquiry-based approaches. Since VCLs do not require physical network connections, it is easier to create network topologies in VCLs to support collaborative learning. Students can be granted full administrative rights on VMs because they are literally "unbreakable" due to the separation of the VM from the workings of the actual physical computer hosting it. Students therefore have the ability to create, configure and network VMs without prior configuration or restriction. This flexibility enables instructors to design more comprehensive problem-based hands-on activities. Although VCLs have the capability to facilitate collaborative learning, the literature focuses mainly on the technological aspects of VCLs as summarized in Table 1. With few exceptions, VCLs have not been evaluated in terms of their pedagogical potential to promote collaborative learning. This paper aims to address this gap in the literature. The objective of this paper is to discuss the benefits of virtual computer laboratories as a collaborative learning environment and present the utilization of collaborative learning strategies for VCLs to enhance student learning.

We have utilized a virtual computer laboratory, the Collaborative Virtual Computer Laboratory (CVCLAB), in several face-to-face and online information security courses at Penn State University's Berks Campus since 2009. In this paper, we first introduce the latest version of the CVCLAB and present an empirical study to demonstrate the benefits of collaborative learning in a VCL.

II. Description of the CVCLAB

At Penn State University - Berks, we established a virtual computer laboratory called the Collaborative Virtual Computer Laboratory (CVCLAB) to create an environment where information security students can meld theoretical knowledge of information security with practical "hands-on" experience. The first prototype of the CVCLAB was built in 2009 and funded by a grant from the Department of Labor through the Wall Street West project. Over the years, we have improved the CVCLAB to support various hands-on activities. The CVCLAB was founded with the following objectives:

- **Enhance the pipeline of information assurance and security employees to industry through outreach and continuing education:** In order to recruit and train future information security professionals programs, we have organized information security themed discovery programs for K-12 students. In these programs, K-12 students use the CVCLAB and its activities to learn about information security[19, 20].
- **Online education and training in information security:** The CVCLAB is remotely accessible from anywhere at any time. Currently, we use the CVCLAB as the main delivery medium for two online asynchronous information security courses[21].
- **Resource Sharing:** The CVCLAB is not only used by Penn State University - Berks students, but also students from other institutions. We have disseminated the blue-print of the CVCLAB to increase collaboration and encourage educational technology transfers among higher education institutions.
- **Support for Collaborative Learning and Inquiry-based Learning:** Supporting collaborative and inquiry-based learning has been one of the primary objectives in the design of the CVCLAB. Many of the hands-on activities developed for the CVCLAB are

designed for collaborative work. We have also shown that inquiry-based activities enhance student learning in the CVCLAB[22].

In the current state, the CVCLAB consists of four different types of VCL designs: Basic Networking and Security, Advanced Networking and Security, Virtual Sandboxes, and Virtual Software Laboratory. Each of these VCL designs has unique topologies and tools as described by Konak and Bartolacci[23] to support various learning objectives. Students can access these VCLs via a web browser or a client interface from anywhere utilizing an Internet connection. In the past year, we have created a new VCL design, the Cyber Security Laboratory, combining the features of the Advanced and Basic Networking and Security VCLs. The topology of the Cyber Security Laboratory is given in Figure 1. In the default configuration of the Cyber Security Laboratory, each user is assigned to four different types of VMs: Windows 7, Windows Server 2008, Backtrack Linux, and Kali Linux. Instead of connecting all VMs through a single virtual network, they are organized into three virtual Local Area Network (LAN) segments connected through a router. LAN1 and LAN2 include student VMs, while LAN3 consists of target VMs, some of which are configured with security flaws. This topology allows us to simulate more realistic network configurations and enables more advanced hands-on activity capabilities. In addition, student teams can take on roles such as attackers and defenders in different network segments. Currently, the Cyber Security Laboratory supports 30 concurrent users and 120 VMs (four VM for each users). Table 2 lists the hands-on activities available for Cyber Security Laboratory.

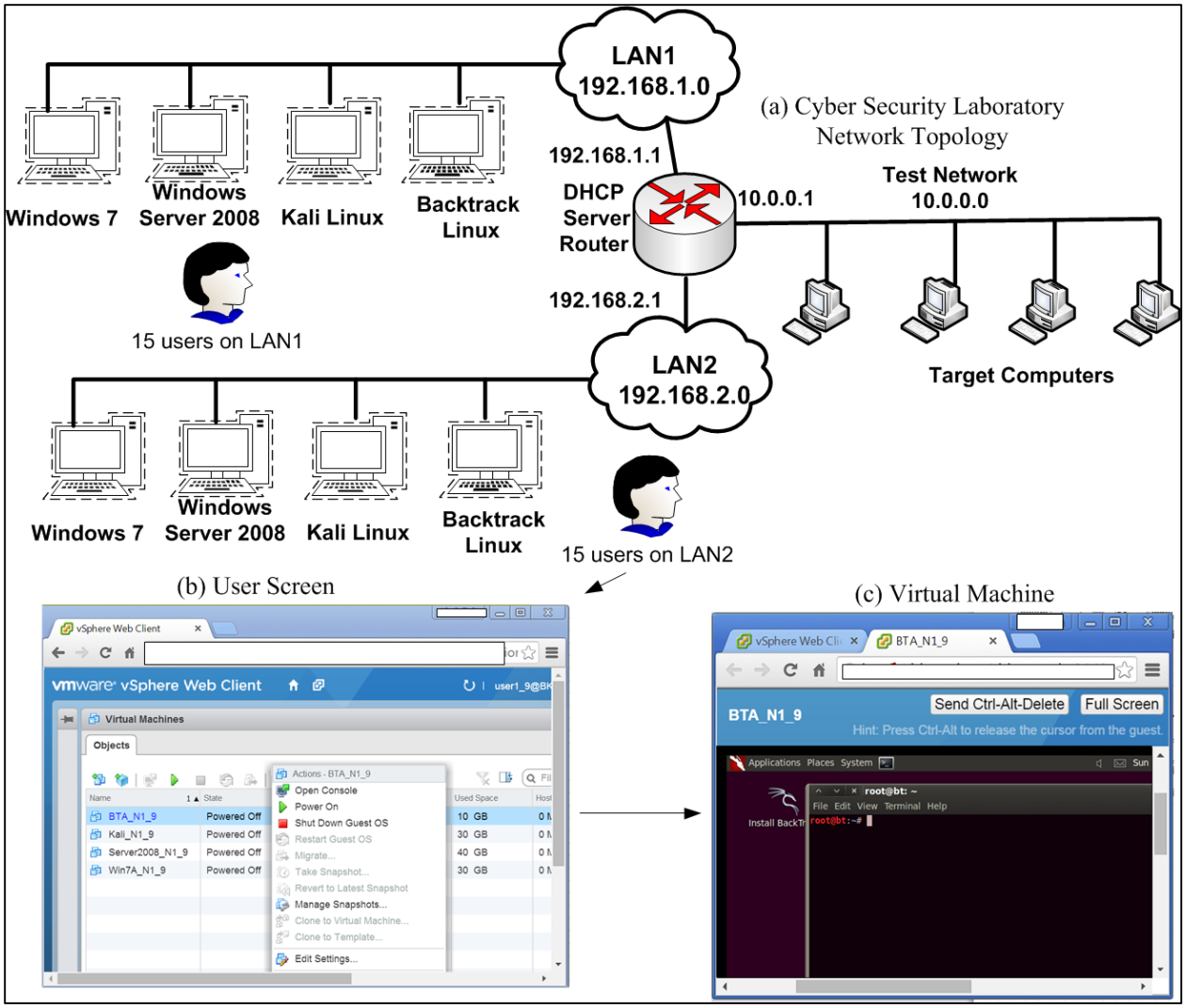

Figure 1. Cyber Security Laboratory Network Topology and Web Client User Access Interface

The Cyber Security Laboratory was implemented using VMWare vSphere 5.5 technology and hosted by several Intel(R) Xeon(R) CPU E5-2650 servers, each with 32 cores, 64GB Memory, and eight network interface cards. The total resource pool dedicated includes 215 Ghz CPU, 281 GB Memory, and 10TB network attached storage. The virtual environment is centrally managed through a dedicated VMware vCenter Server. With its hardware, the Cyber Security Laboratory is highly reliable and provides a robust user experience with minimum latency.

Table 2. Hands-on activities available for the Cyber Security Laboratory

Topic	Hands-on Educational Material Topics
Foundation of Computer Networking	Configuring TCP/IP (Windows and Linux); Network Addressing (IP, MAC, Ports, ARP); Network Management and Diagnostic Tools;
Cryptography	OpenSSL; Traditional and Modern Ciphers; Symmetric and Asymmetric Algorithms; Public Key Infrastructure; Key Exchange; Hashing;
Internet Security Technologies	Digital Signatures; Digital Certificates; Authentication and Authorization;
Internet Security Protocols	Application Layer Security: Pretty Good Privacy (PGP); Transport Layer Security: Secure Socket Layer (SSL); Network Layer Security: Virtual Private Networks (VPN); Internet Protocol Security (IPsec); and Secure Shell (SSH);
HTTP and Web Server Administration	HTTP Protocol; Web Server Administration and Information Services (IIS); Apache HTTP Server and Administration;
Web Server Security	Footprinting; Denial of Service Prevention; Network Mapping and Scanning; Apache Web Server Security Best Practices;
Web Application Security	Input Validation Threats; SQL Injection; Session Management Threats; Man-in-the-Middle Attacks;
Penetration Testing	Target Discovery and Enumeration; Vulnerability Assessment;
Network Attacks	Spoofing: IP and MAC Addresses; Denial of Service Attacks; Password Attacks; Privilege Escalation;
Protecting Networks	Configuring and Securing Routers; Firewalls;
Protecting Windows Hosts	User Accounts and File Permissions; Local Security Policy; Group Policy; Domain Group Policy; Windows Services; Windows Firewall;
Protecting Linux Hosts	Linux Accounts and Permissions; Linux Services and Processes; TCP Wrapper; IP Tables;
Intrusion Detection	Honeypot; Host-Based Intrusion Detection System; Network-Based Intrusion Detection System;

III. A Case Study: Impact of Collaborative Learning in the CVCLAB

Collaborative learning has become an effective approach to providing hands-on skills and knowledge acquisition to students. A flawed and uninspired approach to providing hands-on activities is to give students a step-by-step or "cookbook" assignment to complete that gives little insight into the processes or concepts involved in its completion. In such cases, a hands-on activity can easily turn into a mundane algorithmic sequence of activity steps that students undertake without grasping the motivation and reasoning behind each part of the process. In the CVCLAB, collaborative learning is defined as two or more students attempting to learn a topic

together and creating a product of their learning as they are engaged in a common activity. Some of the benefits of collaborative learning previously described in the literature are as follows:

- Promoting positive effects on student attitudes towards learning and the subject matter.[24,13, 25]
- Promoting critical thinking skills, developing a social support system for learning, reducing of learning anxiety, and building self-esteem in the learner.[26]
- Achieving a higher level of abstract knowledge as a result of collaborative problem solving than individual problem solving.[27]
- Enabling peer scaffolding.[28]
- Increasing problem solving skills.[29]

In this case study, we empirically investigate the benefits of collaborative learning in the CVCLAB. Our main research question is whether collaborative hands-on activities lead to higher student satisfaction versus individual hands-on activities in the CVCLAB.

Hands-on Activity & Participants

We designed the group work (GW) and individual work (IW) versions of a basic computer networking activity to collect data. In the GW version, two students were assigned to two virtual computers, and then they were instructed to configure their computers' TCP/IP settings according to the different scenarios and to test the connectivity between the virtual computers for each scenario. In some scenarios, the virtual computers could not establish a TCP/IP connection, and the students were expected to figure out the reasons for connection problems. In the IW version, a student was assigned to two virtual computers and made all configuration changes and tested the connection between the computers for each scenario. The overall learning objective of this activity was to describe different components of IP address, IP address classes, and sub-/super-netting. The participants of the activity were first year students enrolled in introductory computer networking and introductory information systems classes. Although the activity was not technically difficult (i.e., students were easily able to follow the steps), we observed that some students had difficulty understanding some abstract concepts such as sub-networks.

Data Collection Instrument and Factor Analysis

At the end of the activity, students were asked to evaluate the activity using a questionnaire. The primary objective of the questionnaire was to measure students' overall learning experience (e.g., engagement, challenge, interactions) and their perceived learning outcomes (e.g., competency and interest development). The questionnaire also included questions to measure overall satisfaction with the CVCLAB and the activity. These questions were operationalized with a seven-point Likert scale, ranging from "Strongly Agree" (1) to "Strongly Disagree" (7). In addition, two open-ended questions were included to ask students about what they liked and disliked the most about the activity. The total number of survey participants was N=161. The number of cases in the GW and IW versions were N_{IW}=55 and N_{GW}=106, respectively.

We performed a factor analysis to identify the underlying factors measured by the questionnaire using the extraction method of Maximum Likelihood and the rotation method of Promax with Kaiser Normalization. We did not use the questionnaire items if they had a coefficient lower

than 0.5. The pattern matrix of the seven extracted latent variables and the corresponding questionnaire items are given in Table 3. The meanings of the extracted latent variables are as follows:

- Motivation (MOT): The motivation latent variable measures overall student motivation to complete the activity.
- Interaction (ACT): The interaction latent variable is a measure of the extent to which students interacted with one another during the activity. Note that the students in the IW group were also allowed to interact.
- Reflection (REF): The activity included review and conceptualization questions. This latent variable intends to measure the contribution of these reflective questions to the perceived learning of students.
- Competency (COM): This latent variable is a measure of students' perceived skill improvement as a result of the activity.
- Interest (INT): The interest latent variable intends to measure the level to which students' interest in the subject matter was increased as a result of the activity. This is an important learning objective of the CVCLAB.
- Challenge (CHA): This is a measure of students' perceived difficulty to complete activity.
- Usefulness (USE): This latent variable measures the degree to which students believed that the activity was a useful learning experience.

Table 3. The pattern matrix of the seven extracted latent variables.

Questions	Factor						
	MOT	ACT	REF	COM	INT	CHA	USE
I was very motivated for completing the activity.	.924						
I would like to do more of similar activities	.844						
I found the activity to be interesting.	.838						
Interacting with other students helped me complete the activity.		.973					
The activity encouraged me to ask questions to others.		.855					
I learned new concepts/skills by interacting with other students.		.742					
The activity provided opportunities to reflect back what was learned in the activity.			.901				
The activity promoted helpful discussions about what was performed in the activity.			.869				
The review questions were helpful to reinforce what was performed in the activity.			.742				
The activity improved my technical skills and competency in the subject area.				1.052			
The activity helped me improved my problem solving skills.				.581			
The activity encouraged me to learn more about this topic.					1.064		
The activity increased my curiosity and interest in this area.					.640		
I was encouraged me to use virtual computers in other areas.					.543		
The activity review questions were difficult and time consuming.						.804	
The activity was challenging.						.734	
The time I spent for the activity was worthwhile.							.802
I find the activity useful to me.							.532

Table 4 summarizes the statistics of the factor analysis. Overall, the seven extracted latent variables fitted to the collected data somewhat weakly. However, the grouping of the questions was logical. It should be also noted that the extracted latent variables and grouping of the questionnaire items are very close to the ones used in our previous study[30] in which we could not establish a goodness-of-fit measure due to the low number of cases. Note that factor analysis requires a large number of samples (typically larger than 200) to establish the robustness of the fitted model. The sample size of N=161 can be considered fair to good to build factor models.[31]

Table 4. Statistics of the Factor Analysis

Test		Test Values	Minimum Target Values
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.870	>0.6
Bartlett's Test of Sphericity	Approx. Chi-Square	1944.940	
	df	153	
	Significance	.000	< 0.05
Goodness-of-Fit Test	Chi-Square	64.919	
	df	48	
	Significance	0.052	>0.05

Comparison of Extracted Latent Variables and Discussions

After mapping of the questionnaire items into the latent variables, the latent variable values were calculated by averaging their related question ratings for each case. We used the *t*-test to compare the differences between the latent variable means as well as the overall ratings of the CVCLAB and the activity across the groups. Table 5 summarizes the descriptive statistics for the latent variables, the average ratings of the CVCLAB, and the average ratings of the activity for the two versions of the activity. In addition, the *p*-values of the *t*-tests are provided.

Students rated the CW version of the activity higher than the IW version (*p*-value=.073). They also rated their experience with the CVCLAB significantly higher for the GW version compared to the IW version. It is an unexpected result that students' experience of the CVCLAB was affected by the version of the activity. The significant difference in the ratings of the CVCLAB between the two versions could be due to the peer scaffolding effect of group work. Most of the students used the CVCLAB for the first time during the activity, and the concept of virtualization was new to them. In the GW version, students could support each other to navigate the user interface of the CVCLAB, leading a better user experience.

There was no statistically significant difference between the perceived challenge of the activity across the versions (*p*-value=.476). The students in the GW group indicated higher level motivation than ones in the IW group, but the difference was not statistically different (*p*-value=.184). These results also indicated that both student groups had a similar technical skill set and similar levels of motivation to complete the activity.

As expected, students rated their perceived interaction much higher for the GW version than the IW version (*p*-value=.000). Although both versions of the activity included the same set of reflection questions, the students in the GW version indicated a higher level of reflection than ones in the IW version (*p*-value=.094). The GW group also found the activity more useful (*p*-

value=.069), indicated that their interest in the topic increased more (*p*-value=.021), and gained a greater level of competency (*p*-value=.165) when compared to the IW group.

In particular, the higher level of increased interest of the GW version is notable. To keep up with the fast evolving IT, students are expected to grow as independent learners. However, it is the consensus of our faculty that first year students do not have the mindset for professional growth and independent learning as yet. They have not developed a strong individual and professional interest in the various knowledge areas of information security to motivate them for independent learning outside of the classroom. One objective of the CVCLAB is to increase students' interest in information security fields such that they will be encouraged to use the system independently to study more advanced topics. The results in this study show that group work is more effective in achieving this objective.

Table 5. Comparison of the Latent Variables Across the Activity Versions: Scale: "Strongly Agree" (1) and "Strongly Disagree" (7).

Latent Variable	Treatment	Mean	Std. Deviation	p-value
Activity Rating	IW	3.66	1.23	.073
	GW	3.30	1.11	
CVCLAB Rating	IW	3.24	1.19	.027
	GW	2.80	1.14	
MOT	IW	2.79	1.17	.184
	GW	2.56	.994	
USE	IW	2.94	1.17	.069
	GW	2.58	1.16	
REF	IW	2.85	.964	.094
	GW	2.58	.951	
COM	IW	2.89	.862	. 165
	GW	2.66	1.00	
ACT	IW	3.72	1.68	.000
	GW	2.51	1.05	
INT	IW	3.02	1.27	.021
	GW	2.58	1.03	
CHA (reversed rating)	IW	4.34	1.51	.476
	GW	4.16	1.49	

In summary, collaborative learning in the CVCLAB has been shown to be more beneficial to students. The findings in this paper support that students can develop a higher level of interest as a result of a collaborative hands-on activity than an individual hands-on activity in virtual computer laboratories. Based on the findings in this paper, we recommend that virtual computer laboratories should be designed and used considering the benefits of collaborative learning.

IV. Conclusions

Based on the findings of the work described here, it is our recommendation that Virtual Computer Laboratories are to be designed and utilized for group hands-on activities that can reap the benefits of collaborative learning. In contrast to previous work in the literature that focused on the design aspects of a VCL, we sought to ascertain how the design and use of such laboratories can be used to foster learning. In particular, we showed that hands-on activities and

the actual laboratory setups themselves were both better received by students who were able to collaborate. We recommend that VCLs should be designed and used in consideration of the benefits of collaborative learning. This main contribution from our work demonstrates that social interaction when combined with a hands-on activity that is designed specifically for collaboration, can foster learning using VCLs. In summary, VCLs should be designed as a learning environment that allows students to construct knowledge and skills through a social process.

Acknowledgments

This paper is based on work supported by The National Science Foundation under Award No. DUE-1044800. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

1. Dimkov, T., Pieters, W. and Hartel, P. (2011). *Training students to steal: a practical assignment in computer security education*. Proceedings of the 42nd ACM Technical Symposium on Computer science education, ACM,21-26.
2. Pashel, B. A. (2006). *Teaching students to hack: ethical implications in teaching students to hack at the university level*. Proceedings of the 3rd annual conference on Information security curriculum development, ACM,197-200.
3. Bratosin, B. A. (2014). Cyber Defense Exercises and their Role in Cyber Warfare. *Journal of Mobile, Embedded and Distributed Systems* 6(2), 70-76.
4. Mirkovic, J., Reiher, P., Papadopoulos, C., Hussain, A., Shepard, M., Berg, M. and Jung, R. (2008). Testing a collaborative DDoS defense in a red team/blue team exercise. *Computers, IEEE Transactions on* 57(8), 1098-1112.
5. Schepens, W. J., Ragsdale, D. J., Surdu, J. R., Schafer, J. and New Port, R. (2002). The Cyber Defense Exercise: An evaluation of the effectiveness of information assurance education. *The Journal of Information Security* 1(2).
6. Anisetti, M., Bellandi, V., Colombo, A., Cremonini, M., Damiani, E., Frati, F., Hounsou, J. T. and Rebeccani, D. (2007). Learning Computer Networking on Open Paravirtual Laboratories. *IEEE Transactions on Education* 50(4), 302-311.
7. Bhosale, Y. S. and Livingston L M, J. (2014). V-Lab: A Mobile Virtual Lab for Network Security Studies. *International Journal of Computer Applications* 93(20), 35-38.
8. Briner Jr, J. V., Roberts, J. E. and Worthy, F. (2005). Teaching Computer Science at a Small University. *Association of Small Computer Users in Education (ASCUE)*.
9. Bullers, W. I., Burd, S. and Seazzu, A. F. (2006). *Virtual machines-an idea whose time has returned: application to network, security, and database courses*. Proceedings of SIGCSE '06 Proceedings of the 37th SIGCSE technical symposium on Computer science education Houston, TX, USA,102-106.
10. Li, C. (2006). Lab Development for Delivering Information Systems Courses Online at Small Campuses. *Journal of Cases on Information Technology (JCIT)* 8(1), 15 pages.
11. Gaffer, S. M. and Alghazzawi, D. M. (2012). Using Virtual Security Lab in Teaching Cryptography. *International Journal of Modern Education and Computer Science (IJMECS)* 4(1), 26.
12. Garcia, C. R., Quesada, A., Candela, S., Carrasco, E. and Gonzalez, A. (2012). *Using a virtual and hosted lab for information systems technologies*. Global Engineering Education Conference (EDUCON), 2012 IEEE, IEEE,1-9.
13. Hamada, M. (2008). An integrated virtual environment for active and collaborative e-learning in theory of computation. *IEEE Transactions on Learning Technologies* 1(Copyright 2009, The Institution of Engineering and Technology), 117-130.
14. Hu, J., Cordel, D. and Meinel, C. (2005). *Virtual machine management for tele-lab" IT-Security" server*. Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE Symposium on, IEEE,448-453.

15. Kneale, B., De Horta, A. Y. and Box, I. (2004). *VELNET: Virtual Environment for Learning Networking*. ACE '04 Proceedings of the Sixth Australasian Conference on Computing Education, Dunedin, New Zealand,161-168.
16. Tran, N. H., Tran, H. D., Chiem, P. T., Luu, D. T., Cao, T. D. and Kaskenpalo, P. (2013). *CenLavi: Virtual Computer Network Laboratory*. Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on, IEEE,523-528.
17. Son, J., Irrechukwu, C. and Fitzgibbons, P. (2014). Virtual Lab for Online Cyber Security Education. *Communications of the IIMA* 12(4), 5.
18. Wright, J., Carpin, S., Cerpa, A., Gavilan, G., Kallmann, M., Laird, C., Laird, K., Newsam, S. and Noelle, D. (2007). *Collaboratory: An Open Source Teaching and Learning Facility for Computer Science and Engineering Education*. FECS, 368-373.
19. Konak, A. (2014). *A cyber security discovery program: Hands-on cryptography*. Integrated STEM Education Conference (ISEC), 2014 IEEE,1-4.
20. Nasereddin, M., Clark, T. K. and Konak, A. (2014). *Using virtual machines in a K-12 Outreach program to increase interest in information security fields*. Integrated STEM Education Conference (ISEC), 2014 IEEE,1-5.
21. Konak, A. and Ryoo, J., and Kulturel-Konak, S. (2014). *Student Perceptions of a Hands-on Delivery Model for Asynchronous Online Courses in Information Security*. ASEE Mid-Atlantic Section Fall 2014 Conference, Swarthmore College, Swarthmore, PA,1-7.
22. Konak, A., Clark, T. and Nasereddin, M. (2014). Using Kolb's Experiential Learning Cycle to Improve Student Learning in Virtual Computer Laboratories. *Computers & Education* 72, 11-22.
23. Konak, A. and Bartolacci, M. R. (2012). *Broadening E-Commerce Information Security Education Using Virtual Computing Technologies*. the 2012 Networking and Electronic Commerce Research Conference, Riva Del Garda, Italy,6 pages.
24. Lou, Y., Abrami, P. C. and d'Apollonia, S. (2001). Small group and individual learning with technology: A meta-analysis. *Review of educational research* 71(3), 449-521.
25. Johnson, D. W., Johnson, R. T. and Stanne, M. B. (2000). Cooperative learning methods: A meta-analysis.
26. Laal, M. and Ghodsi, S. M. (2012). Benefits of collaborative learning. *Procedia-Social and Behavioral Sciences* 31, 486-490.
27. Schwartz, D. L. (1995). The emergence of abstract representations in dyad problem solving. *The Journal of the Learning Sciences* 4(3), 321-354.
28. Wass, R., Harland, T. and Mercer, A. (2011). Scaffolding critical thinking in the zone of proximal development. *Higher Education Research & Development* 30(3), 317-328.
29. Kuo, F.-R., Hwang, G.-J., Chen, S.-C. and Chen, S. Y. (2012). A Cognitive Apprenticeship Approach to Facilitating Web-based Collaborative Problem Solving. *Educational Technology & Society* 15(4), 319-331.
30. Konak, A., Bartolacci, M. and Huff, H. (2012). *An Exploratory Factor Analysis of Student Learning in a Collaborative Virtual Computer Laboratory*. Proceedings of AMCIS 2012 Seattle, WA, paper 23.
31. Comrey, A. L. and Lee, H. B. (2013). *A first course in factor analysis*: Psychology Press.