

Designing of Virtual Cloud Labs for the Learning Cisco CyberSecurity Operations Course

Nadiia Balyk^[0000-0002-3121-7005], Yaroslav Vasylenko^[0000-0002-2954-9692],
Vasyl Oleksiuk^[0000-0003-2206-8447] and Galina Shmyger^[0000-0003-1578-0700]

Ternopil Volodymyr Hnatiuk National Pedagogical University
2, M. Kryvonosa St., Ternopil, 46027, Ukraine

{nadbala, yava, oleksyuk, shmyger}@fizmat.tnpu.edu.ua

Abstract. The article is devoted to the study of the problem of the cybersecurity basics teaching. The training of the ICT-specialties students using the course “CCNA Cyber Operations” of the network academy Cisco is considered. At present, many universities have similar academies, while others can open them. On the basis of free software platforms Apache CloudStack and EVE-NG Community authors designed and implemented a virtual cloud laboratory. It operates according to the “IaaS” model. Thanks to the technology of embedded virtualization, the work of many virtual machines, storing of their status, traffic analysis and visualization of network topologies are maintained.

The article describes the experience of teaching students of the specialty “Pedagogical education. ICT” in the course “CCNA Cyber Operations” with the use of virtual cloud laboratories. The authors have been conducted a survey of students who studied at the course. Its purpose was to determine how much they satisfied were with the course. Statistical processing of the results was performed on the basis of the Rasch model using the software MiniSteps.

Keywords: ICT-competence, virtual cloud lab, Apache CloudStack, EVE-NG Community, computer science trainee teachers, Rasch model.

1 Introduction

Today, the development of computer networks provides almost universal access to information resources. Along with the positive, there are negative consequences – interference with private life, theft or destruction of the personal or corporate data. Many people are unaware that when browsing Internet sites, it is possible to process and store their personal data and transactions not only by web page developers, but also by outsiders. Massive data collection through social networks, profiling of the viewing of information resources creates the effect of the “digital shadow” of a person [14].

Solving the problem is possible provided the development of information security competencies. At present, many universities in Ukraine are preparing specialists in the field of cybersecurity. However, this process must be continuous and start at school.

In this context, the teaching of informatics teachers on the basics of cybersecurity is an important problem. One way to solve this problem is to study open courses by students. Their advantages are as follows: the opportunity to study at a convenient time; the ability to compare teaching styles and materials of different courses; the experience in discussing and peer assessment; improving the skills of listening, reading and writing English (or other); reflection of their own pedagogical activity in the light of new ideas, the digital creativity and collaboration with other participants [9].

Cisco offers similar courses within Cisco Network Academy. Although these courses do not fully correspond to the ideology of the MOOC, Cisco Network Academy can be organized at virtually any university. Cisco Networking Academy, a Cisco Corporate Social Responsibility Program, is an IT skills and career building program available to educational institutions and individuals worldwide.

The goal of this article is to design the virtual cloud labs for formation teachers' competences in cybersecurity and to research the efficiency of such labs..

2 Presentation of the main results

As the experience of a secondary school shows, a teacher of informatics is the leading ICT specialist [1]. In the context of providing information security, he must be able to balance the advantages and disadvantages of using network technologies in the learning process. Having analyzed the available free courses, we chose CCNA Cyber Operations [4] as a basic course for formation teachers' cybersecurity competences. By the end of this course, the students will be able to:

- Install virtual machines to analyzing cybersecurity threat events.
- Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- Explain the Windows and Linux OS features to support cybersecurity analyses.
- Analyze the operation of network protocols and services.
- Classify the various types of network attacks and identify network security alerts.
- Use network monitoring tools to identify attacks against network protocols.
- Use various methods to prevent malicious access to computer networks.
- Apply incident response models to manage network security incidents.

The course contains the following chapters: Cybersecurity and the Security Operation Center, Windows OS, Linux OS, Network Protocol and Services; Network Infrastructure, Principles of Network Security, Network Attacks: A Deep Look, Protection the network, Cryptography and the Public Key Infrastructure, Endpoint Security and Analysis, Security Monitoring, Intrusion Data Analysis, Incident.

Each chapter of this course contains terms and concepts review, quiz, labs and exam. In the process of teaching the course, we met with the problem of organizing laboratory works. Cisco Network Academy offers to run them on virtual student machines. This approach is justified, but it limits the universal and everywhere access of students to study. The use of separate virtual machines does not ensure the cooperation of students between themselves and with the teacher.

An effective way to overcome these limitations is to use the cloud technologies. The authors [11] note that the development of cloud computing technologies, adaptive information and communication networks services, virtual and mobile learning facilities are the important step towards solving the problems of accessibility and quality of training. Application of cloud technologies in professional activities should correspond the requirements of fundamentalization of learning through the inclusion in the content general both the theoretical and the technological provisions, with demonstration of them on the concrete examples [6]. M. Shishkina and O. Glazunova distinguishes the following levels of the University Cloud-based Learning and Research Environment: physical, level of the virtualization and virtual resource management, as well as platforms and software levels [5].

We deployed a cloud-based environment according to the IaaS model. In the environment, the public and private cloud platforms are integrated. Since the corporate cloud platforms are widely using the virtualization technology, we see as possible the deployment of virtual training laboratories on their basis.

After analyzing the interpretation of V. Bykov, we note that the virtual laboratory is an information system in which network virtual ICT objects are formed thanks to a special user interface, which is supported by the system software of the network setting. Such objects are an integral part of a logical network infrastructure with a flexible architecture that, according to its structure and time, corresponds to the personality needs of the user [3].

Typically, in a virtual laboratory, information from a subject field is based on some facts, and therefore limited by a set of predicted experiments. Another approach suggests that a pupil or student is able to carry out any experiments, not limited to a previously prepared set of results. It is thanks to the use of the virtualization technology of operating systems, the last approach should be tried to implement in the designed laboratory. Cloud technologies and virtualization technology provide unique opportunities for the learning organization of the Cisco CyberSecurity Operations course.

The designed virtual laboratory was implemented in the cloud-based learning environment of Volodymyr Hnatiuk Ternopil National Pedagogical University. Based on the comparative analysis [8], as the program basis of the laboratory, we have chosen the Apache CloudStack platform. Then we modified the Cloud-based Learning Environment so that students could create virtual networks. This networks should not require changes in the topology of physical networks in the academic cloud. We divided the traffic transmitted between students' virtual computers among 100 VLANs. So each student has an opportunity to store their virtual computers and other devices in their personal or several guest networks.

As Apache CloudStack does not provide tools for visualization of network structure, students often have difficulty in designing and configuring networks in a cloud infrastructure. That fact prompted us to integrate into a virtual cloud laboratory a system that makes it possible to visualize the process of network design. It was vital that such system could work with networks on Apache CloudStack virtual machines. We analyzed relevant publications and compared several platforms – Cisco packet tracer, Graphical Network Simulator (GNS), Unetlab (EVE-NG). Despite the benefits

of Cisco packet tracer, it did not provide the performance of all tasks of the laboratory works. Among the platforms of GNS and EVE-NG, we have chosen the last.

Every student's copy of ENE-NG platform is a separate virtual machine in Apache CloudStack cloud. As each node of EVE-NG is itself a virtual machine, hosts integrated in Apache CloudStack infrastructure have to support nested virtualization.

The laboratory works involves the use of such virtual machines: CyberOps WorkStation (based on Arch Linux); Kali Linux; Security Onion (based on Ubuntu Linux); Metasploitable; Windows Client.

The students used a virtual cloud laboratory when performing the laboratory works of following chapters: Windows Operating System, Linux Operating System, Network Protocols and Services, Network Attacks, Intrusion Data Analysis [Ошибка! Источник ссылки не найден.].

A typical topology of the network for the laboratory works is showed on Figure 1.

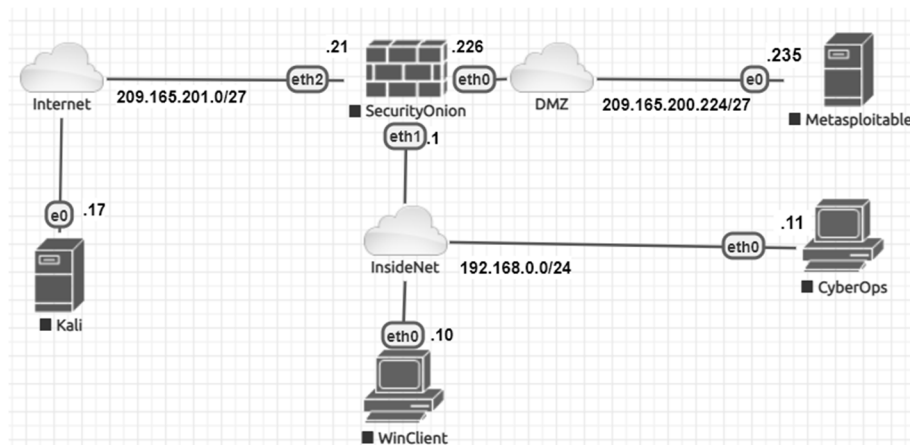


Fig. 1. The network topology for labs

Each of these machines was available in a cloud-based infrastructure. As a result, students could work with virtual machines in the university's local network or through VPN. The course was taught in a mixed methodology. It was dominated by independent distance work of students. The teacher's consultations were carried out at the classroom and online.

After learning the course, students completed the final exam. He contained 60 questions from all the topics of the course, as well as the fragments of laboratory works. 56 students majoring in "Pedagogical education. ICT" passed the exam. Of these, only 24 passed the exam successfully (75% points and more). This indicator can be explained by the fact that the course "Cyber Operations" was studied as optional and did not affect the student's rating at the university.

In addition to the final exam students responded to the questionnaire "CyberOps Course Feedback". Questionnaire questions were formulated according to the principle of the Likert scale (five response categories) and grouped in 5 blocks [10].

3 Statistical analysis of research data

To evaluate the efficiency of the designed and deployed cloud-based environment, a model with equally distributed responses of all indicators on the scale of the latent variable was used. This is one of the models of the Rasch's family, which is used in the case of polithomus indicators. The Rasch's model is interpreted as a model of "objective measurements" that do not depend from the respondents and measuring instruments [2].

To measure the complexity of tasks and level of knowledge, the unit of measurement, called logit, is used. In our research, we used the WINSTEPS program (USA). The program is commercial, but its free version called MINISTEP. It allows you to use all the capabilities of WINSTEPS, but has a limit on the number of questions in the test (25) and the number of people (75) [15].

Standardized Residuals in the Rasch's model are modeled for normal distribution. Therefore, significant deviations from the value of "0" for the Mean and the "1" for the Standard Deviation (SD) signal that the primary data do not correspond to the Rasch's model, which should correspond exactly to the normal distribution. In our study, the values Mean = -0.02 and SD = 1.03 are sufficiently satisfactory.

Reliability of the survey scale. The classic indicator of reliability of the survey scale is alpha Kronbach. Professionally designed tests must have an internal consistency of at least 0.90. In our survey, the Cronbach coefficient $\alpha=0.96$.

As can be seen from Figure 2, informational and characteristic functions are acceptable for IRT (Item Response Theory) analysis.

Table 1. Output table "Summary Statistics" (summary of 56 measured person)

	Total Score	Count	Measure	Model S.E.	INFIT		OUTFIT	
					MNSQ	ZSTD	MNSQ	MNSQ
MEAN	72.1	25.0	-0.20	0.25	1.06	-0.13	1.07	-0.14
SEM	2.9	0	0.18	0.00	0.08	0.29	0.09	0.29
P.SD	21.5	0	1.30	0.03	0.62	2.27	0.65	2.14
S.SD	21.6	0	1.31	0.03	0.63	2.19	0.66	2.16

Person raw score-to-measure correlation = 1.00.

Cronbach Alpha (kr-20) person raw score "test" reliability = 0.96, sem = 4.07.

Table 2. Output table "Summary Statistics" (summary of 25 measured item)

	Total Score	Count	Measure	Model S.E.	INFIT		OUTFIT	
					MNSQ	ZSTD	MNSQ	MNSQ
MEAN	161.6	56.0	0.00	0.17	0.98	-1.13	1.07	-0.80
SEM	2.5	0	0.07	0.00	0.17	0.83	0.19	0.88
P.SD	12.2	0	0.34	0.00	0.84	4.08	0.95	4.32
S.SD	12.4	0	0.35	0.00	0.85	4.16	0.97	4.41

Item raw score-to-measure correlation = -1.00

In columns INFIT and OUTFIT Tables 1, 2 specified parameters that characterize the correspondence of the data to Rasch's model. In the field MNSQ (mean-square statistic) the statistics of the correspondence of the output data to the measuring model are showed, obtained on the base of the average sums of the squares of the deviations of the theoretical values from the empirical ones. The most qualitative and significant (productive) measurements are those for which the MNSQ values lie in the range of 0.5 to 1.5. In the ZSTD field, the standardized MNSQ values are showed (with an average of 0 and a standard deviation of 1). Valid value is $-2.0 \leq ZSTD \leq +2.0$. For this survey, the match statistics for the measurements of all items are in these ranges, so they can all be used for further analysis.

Figure [12] shows the distribution of respondents and their judgments on the same interval scale (efficiency of the designed and deployed cloud-based environment). The content and composition of the questions in the survey is satisfactory – this is evident from the second bar graph [6].

Table 3. Item Statistics: Measure Order

Entry number	Total Score	Total Count	Measure	Model S.E.	Item
11	135	56	0.75	0.17	CA6
1	147	56	0.41	0.17	CS1
3	149	56	0.35	0.17	CS3
12	151	56	0.29	0.17	CA7
16	151	56	0.29	0.17	CI4
19	154	56	0.21	0.17	CC2
14	155	56	0.18	0.17	CI2
21	156	56	0.15	0.17	CC4
7	157	56	0.13	0.17	CA2
10	159	56	0.07	0.17	CA5
6	160	56	0.04	0.17	CA1
9	160	56	0.04	0.17	CA4
15	160	56	0.04	0.17	CI3
18	160	56	0.04	0.17	CC1
13	161	56	0.02	0.17	CI1
4	162	56	-0.01	0.17	CS4
2	165	56	-0.09	0.17	CS2
17	166	56	-0.12	0.17	CI5
25	168	56	-0.18	0.17	CP4
8	169	56	-0.20	0.17	CA3
5	170	56	-0.23	0.17	CS5
23	172	56	-0.29	0.17	CP2
24	176	56	-0.40	0.17	CP3
22	177	56	-0.43	0.17	CP1
20	200	56	-1.08	0.17	CC3
Mean	161.60	56.00	0.00	0.17	
P.SD	12.20	0.00	0.34	0.00	

By analyzing Table 3 in terms of the distractors included in the poll, the following conclusions can be drawn. Distractors with the lowest estimate of the efficiency of the

proposed medium (Measure = -1.08, Item = CC3) and with the highest estimate of the efficiency (Measure = 0.75, Item = CA6) are not presentational for this study, since on the responses had an impact the factor of randomness and the factor of reluctance of respondents to understand the content of the questions deeply. The rest of the distractors can be divided into three groups according to the degree of influence on the overall efficiency: 1) with a small degree of influence on the overall efficiency (Measure from -0.43 to -0.12, Items = CP1, CP3, CP2, CS5, CA3, CP4, CI5); 2) with a mediocre degree (Measure from -0.09 to 0.07, Items = CS2, CS4, CI1, CC1, CI3, CA4, CA1, CA5); 2) with a large degree of impact on overall efficiency (Measure from 0.13 to 0.41, Items = CA2, CC4, CI2, CC2, CI4, CA7, CS3, CS1). The analysis of these distractors at the content level will allow for the adjustment of the structure, some components in design of virtual cloud labs for the learning Cisco CyberSecurity Operations.

4 Conclusions

Learning the basics of cybersecurity is a topical issue of ICT students training. The course “CCNA Cyber Operations” of Cisco Network Academy provides an opportunity to organize such training. It contains a lot of theoretical materials, quiz tasks, discussion questions, labs, chapters exams and final exam. A virtual cloud laboratory was designed to carry out laboratory works at the course. For this purpose, the Apache CloudStack and EVE-NG Community Edition platforms were used. The virtual cloud laboratory provides the following possibilities: to create the required number of virtual machines; to change the computing power; to simulate the work of real computers and networks; to visualize different network topologies; to keep the state of virtual computers; to work remotely through a virtual private network; to combine separate virtual networks of students into a single network; to help students and control their learning outcomes.

The conducted experimental research and its statistical processing have confirmed by the efficiency of the use of the virtual cloud laboratory. Along with high-quality training materials from the Cisco Network Academy, the students appreciated highly the functional and widespread access to the virtual objects of the cloud lab.

References

1. Bilousova, L., Ponomarova H.: The Role of the Information Technologies Teacher in the of Secondary School Pupils Career Guidance to IT-speciality. Professionalism of the Teacher: Theoretical and Methodological Aspects. 4, 157–166. <http://pptma.dn.ua/index.php/en/archive/archive-2016/issue-4-2016/374-the-role-of-the-information-technologies-teacher-in-the-of-secondary-school-pupils-career-guidance-to-it-speciality> (2016). Accessed 26 Mar 2019
2. Bond, T., Fox, C.: Applying the Rasch Model: Fundamental Measurement in the Human Sciences. Routledge, New York. (2007)

3. Bykov V., Shyshkina, M.: Theoretical and Methodological Principles of the Cloud Based University Environment Formation. Theory and practice of social systems management. 2, 30–52. <http://tipus.khpi.edu.ua/article/view/73497> (2016) Accessed 26 Mar 2019
4. CCNA Cyber Ops - Cisco. <https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-cyber-ops.html> (2019). Accessed 26 Mar 2019.
5. Glazunova, O., Shyshkina, M.: The Concept, Principles of Design and Implementation of the University Cloud-based Learning and Research Environment. In: Ermolayev, V., Suárez-Figueroa, M.C., Yakovyna, V., Kharchenko, V., Kobets, V., Kravtsov, H., Peschanenko, V., Prytula, Ya., Nikitchenko, M., Spivakovsky A. (eds.) Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer (ICTERI, 2018), Kyiv, Ukraine, 14-17 May 2018, vol. II: Workshops. CEUR Workshop Proceedings. **2104**, 332–347. http://ceur-ws.org/Vol-2104/paper_158.pdf (2018). Accessed 26 Mar 2019
6. Information and Characteristic functions. https://docs.google.com/document/d/1L-0hdOwfjSSiub_xEIQCbVMqkvHAbBPIXicUMiW-e8o/edit (2019). Accessed 22 May 2019
7. Markova, O., Semerikov, S., Popel, M.: CoCalc as a Learning Tool for Neural Network Simulation in the Special Course “Foundations of Mathematic Informatics”. In: Ermolayev, V., Suárez-Figueroa, M.C., Yakovyna, V., Kharchenko, V., Kobets, V., Kravtsov, H., Peschanenko, V., Prytula, Ya., Nikitchenko, M., Spivakovsky A. (eds.) Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer (ICTERI, 2018), Kyiv, Ukraine, 14-17 May 2018, vol. II: Workshops. CEUR Workshop Proceedings. **2104**, 338–403. http://ceur-ws.org/Vol-2104/paper_204.pdf (2018). Accessed 26 Mar 2019
8. Oleksyuk, V.: Designing of university cloud infrastructure based on apache Cloudstack. Information Technologies and Learning Tools. **54(4)**, 153–164 (2016). doi:10.33407/itlt.v54i4.1453
9. Panchenko, L.: MOOCs for the Development of the Teacher of the New Ukrainian School. <http://lib.iitta.gov.ua/709942> (2018). Accessed 26 Mar 2019
10. Questionnaire of Cyber Operations Course Feedback. <https://docs.google.com/document/d/1nOeGMi3JgDYdkAt9exJTjLR5YoFIWcdg0Rgo-XKME64/edit> (2019). Accessed 15 May 2019
11. Semerikov, S., Shyshkina, M. (eds.): Cloud Technologies in Education. Proceedings of the Workshop, CTE 2017. CEUR Workshop Proceedings. **2168**. <http://ceur-ws.org/Vol-2168> (2018). Accessed 26 Mar 2019
12. The relationship between the level of efficiency of the designed and deployed cloud-based virtual lab and the indicator variables. <https://docs.google.com/document/d/1vL0C71qNAB11O6aKuJDq5MIT4uPZ114b8K1ysD2JcI8/edit> (2019). Accessed 22 May 2019
13. The topics of work, in the study of which was used virtual cloud laboratory. https://docs.google.com/document/d/1YUqSJpx93nj_X31yeKGzVWNWx9B3PpkKcTri8xH3NOc/edit?usp=sharing (2019). Accessed 15 May 2019
14. van Rooy, D.; Bus, J.: Trust and Privacy in the Future Internet – a Research Perspective. Identity in the Information Society. **3(2)**, 397–404 (2010). doi:10.1007/s12394-010-0058-7
15. WINSTEPS & Facets Rasch Software. <http://www.winsteps.com> (2019). Accessed 26 March 2019