VIRTUALIZATION TECHNOLOGY FOR LABORATORY WORKS BY EXAMPLE OF TEACHING THE DISCIPLINE «WEB RESOURCES PROTECTION»

Belousova E.S.[1], Ignatovich E.S.[2]

[1]*Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus,*
elena1belousova@gmail.com;

[2]*National Institute for Higher Education, Minsk, Belarus,*
alenaignatovitch@gmail.com

Abstract. Ways of introducing virtualization technology into the educational process and an example of teaching laboratory work in discipline «Web Resources Protection» in English are presented. The advantages and features of the application of this technology in distance learning process are highlighted

Introduction. Laboratory work can be defined as learning methods and the form of educational process [1, p.190]. Laboratory work is a method of learning in which students perform experiments or perform practical tasks with the teacher guidance and according to a predetermined plan. They perceive and comprehend new educational materials in the process of their implementation. Laboratory work is a form of organization the educational process, aimed at obtaining practical skills through working with material objects or models of the course subject area.

According to various approaches to the classification of teaching methods, laboratory works include: visual teaching methods; independent work of students in understanding and assimilating new material; educational work on the application of knowledge in practice and the development of skills [2].

Practical work is a key component of engineering degrees and laboratory sessions are one of the principal ways that engineers learn how to apply theory. However, with the increase in class sizes and the drain on resources to provide up-to-date equipment, universities are increasingly using web-based laboratories (also referred to as virtual or remote labs or e-practicals). Virtual labs can also help to develop laboratory skills in distance learning of students and disabled students who may not be able to access traditional laboratories. The practical sessions can use a range of technologies including online movie clips, simulations and labs controlled over the internet. While virtual approaches cannot replace real-world experimentation in technology and engineering, if a sound pedagogic approach is adopted, they can be a valuable aid to understanding [3, p.271].

The aim of the work is to analyze the introduction of virtualization technology in the educational process by the example of teaching laboratory work on the discipline «Web Resources Protection» in English.

Laboratory works on the discipline «Web Resources Protection» are based on virtualization technology, which is also named virtual lab. Using desktop virtualization technology, a decentralized virtual lab approach can be implemented. Students install and run a desktop virtualization software package, like VMware Workstation or Oracle VM VirtualBox, on their notebook computers or personal computers. The prebuilt images are distributed and imported to students' laptop or desktop computers. Students run the prebuilt images (virtual machines) on their machines to complete lab assignments.

Statement of education process. Virtualization allows multiple virtual machines (VMs) to run concurrently on a single computer [4, p.149]. Each virtual machine shares the resources of a single computer. The different virtual machines can run different operating systems and multiple applications in isolation on the same physical machine. Deploying automated virtualization technology, coupled with cloud based access, provide the ability for applications to be dynamically available to end users. Among many different types of virtualization technologies, two virtualization technologies can be deployed for virtual labs:

– server-side virtualization for running the virtual machines on a remote server;

– desktop virtualization (sometimes called client virtualization or decentralized virtualization) for running virtual machines on user's own personal computer.

Server virtualization makes it possible to deploy virtual labs which require high-end equipment and resources. Server side virtualization software creates Virtual Machines (VM) on a remote server (VM host machine). The virtual machine (VMs) is an instance of some operating system platform running on any given configuration of server hardware and managed by a virtualization manager/monitor (also known as a hypervisor). A hypervisor is virtualization software that allows several operating systems (or virtual machines) to share a single hardware host without disrupting each other. Since many different operating systems and applications can run on a single piece of hardware, cost savings and efficiency are among the primary benefits [5, p.84].

Computer class with an individual workplace for each learner, internal computer network and Internet access are required for laboratory work.

According to [6] the information security lab should be divided into three regions: training room, work area and equipment area. The training region is used for training and teaching, which includes platform, screen announcement area, blackboard, projection area and tables. The training room will meet the need of small-group students to do experiments at the same time. The working area is provided for laboratory administrator and teachers. The equipment area is used for placing experimental equipments, including network cabinets, server cabinets and equipment area etc.

The network area is designed for placing various security equipments and network switching equipments; the server cabinet area is designed for placing required servers. The working teacher area can use a projector, security audit system and log audit system to display students' behavior of attack target area.

The virtualized network infrastructure in figure 1 is used as a laboratory layout. This network is implemented in the Oracle VM VirtualBox virtual environment. The network structure contains a web servers (OWASP, LinuxLive01, LinuxLive02) and a personal device from which it is possible to implement vulnerability analysis (Kali).

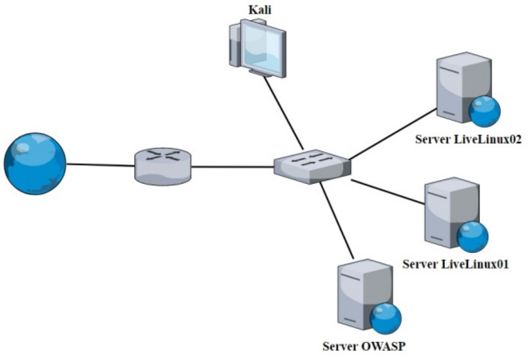

Figure 1 – Virtualized Network Infrastructure

The OWASP server contains a deliberately insecure Java web applications designed to master the security of web applications. This application allows students to learn how to identify vulnerabilities commonly found in Java applications that use common and popular open source components. The OWASP server is based on the Open Web Application Security Project, with a series of lessons that teach different application security measures and penetration testing methods.

LinuxLive01, LinuxLive02 server contains Web For Pentester vulnerable to various types of attacks. The Kali virtual machine contains the Kali Linux operating system, which is a tool primarily aimed at using experienced users to conduct tests to detect vulnerabilities, as well as measures to eliminate them.

For testing some vulnerability students need to use application Burp. Burp is widely used to analyze web application vulnerabilities. It is an integrated platform for performing web application security tests with various tools that work together effectively to support the entire testing process, from mapping a site and analyzing the attack surface of an application to searching and exploiting security vulnerabilities. Burp Suite contains a snooping proxy that allows to inspect and to modify traffic between browser and the target application.

Students can read tasks in the practical part of guidelines for laboratory works, where they can find recommendation for implementation. For a student to perform laboratory work clearly, the guideline describes in detail the sequence of actions for completing the assignment.

Virtualized Network Infrastructure is useful tool for developing students practice skills of web-attack. Also this Infrastructure allows to create any applications of different levels and services. That is why it is important for laboratory classes of discipline «Web Resources Protection».

Discussion of outcomes. After completing of the laboratory work students form reports that describe each step of the attack. They have to fill in the table for describing each step of attack. The report for each step should illustrate actions in the form of screenshots with highlighted vulnerable elements.

Reports are very important and provide the structured detailed of the application test. In professional activities, experts prepare such reports after the engagement has been completed. Once the report is prepared, it is shared among the senior management staff and technical team of target organizations. If any need arises in future, this report is used as the reference. Therefore, it is very important to teach students how to write web application testing reports correctly.

In this way, students acquire scientific knowledge on the basic concepts of web technologies security, familiarize with the technologies of web applications protection, and form the skills to conduct analysis of the security of web applications and the configuration of means of protection against web attacks.

Conclusion. Thus, using of virtualization technologies in the educational process allows not only to reduce funds for the purchase and maintenance of real equipment. The ways of designing effective virtual machine architecture to support information security hands on labs for instruction in a highly scalable and cost effective basis were found. The selected virtual design approach isn't only for providing acceptable performance, but also for providing the users with a consistent environment that is designed to support multiple courses and potentially hundreds of students. This method of teaching laboratory work can be applied not only for classroom activities but for distance learning, because a student can install all necessary programs himself.

References

1. Shirshova, T.A. Laboratory work as a means of motivating and enhancing student learning / T.A. Shirshova, T.A. Polyakova // Omsk Scientific Herald. – 2015. – №4. – P.188–190.

2. Khatsrinova, O.Yu. Laboratory work in an engineering university as a means of motivating students' cognitive activity / O.Yu. Khatsrinova // Bulletin of Kazan Technological University. – 2013. – T.16, №16. – P.259–262.

3. Fry, H.A Handbook for Teaching and Learning in Higher Education Enhancing Academic Practice Third edition. / H. Fry, S. Ketteridge, S. Marshall. – New York : Taylor & Francis e-Library, 2008. – 544 p.

4. Virtualization tools in teaching of IT Disciplines / Vasilyeva I.N., Rodin V.N., Chernoknizhnyi G.M. // Bulletin Of Saint-Petersburg University Of The Mia Of Russia. – 2018. – №1 (77). – P.148–154.

5. Son, J. Virtual Lab for Online Cyber Security Education / J.Son, C.Irrechukwu, P.Fitzgibbons // Communications of the IIMA. – 2012. – Volume 12, Issue 4. – P.81–96.

6. Zhu Li A New Construction Scheme for Information Security Lab / Li Zhu, Huaqing Mao, Zhiwen Hu // Creative Education. – 2012. Vol. 3, No.4. – P.406–412.