Development of Network Security Education

Risto Honkanen, Mikko Myllymäki, and Ismo Hakala
University Consortium Chydenius
University of Jyväskylä
Kokkola, Finland
Email: {firstname.lastname}@chydenius.fi

***Abstract*—Distance education has grown tremendously over the last decade. Internet technologies have enabled a large-scale dispensation of lectures, exercises, and training. Virtual Learning Management Systems (LMSs) offer a number of tools to realize distance education and distance learning. In this work, we present a virtual system architecture for training cyber security professionals with hands-on skills. The architecture is based on a VirtualBox virtualization environment. Guest machines are installed on an instance of VirtualBox. The installed environment offers a safe and isolated workbench for experiments. After installation and configuration of the environment, students perform a number of instances of cyber attacks and system protections. According to students, the experiments were quite challenging but educational.**

***Index Terms*—network security, distance education**

I. Introduction

Attacks on computer systems are a serious and increasing threat. Such attacks may harm users or put their data at risk. Risks are increasing rapidly for at least two reasons. On the one hand, the number of installed Internet devices are growing quickly. Manufacturers are obliged to release new products faster and faster. In some cases, this may be carried out at the expense of safety. On the other hand, it is possible that end users do not recognize the threats posed by cyber attacks. They may use default usernames and passwords, omit firewalls and use of virus scanners, and so on. Therefore, cyber security education is considered very important.

The Network Security course (3–5 ECTS) is compulsory for our master's-level students. This advanced university course is intended to give students experience with installation, configuration, and administration of a computer system, an interactive network security training environment, and experience in protecting a computer system.

The course consists of a number of prerecorded video lectures and 13 self-study exercises divided into three main sections: installation and administration, cyber attacks, and system protection. Prerecorded video lectures provide some basic background information about network security. In the installation and administration section, students learn to install the virtual environment and virtual computers needed in the subsequent exercises. They install Oracle VirtualBox, virtual system servers, and a number of virtual clients and attacker machines. The cyber attacks section introduces various hostile intrusion and cracking techniques, including Address Resolution Protocol (ARP) poisoning, Internet Control Message Protocol (ICMP) redirecting, cracking HTTP pages, and reverse Transmission Control Protocol (TCP) attack. The system protection section focuses on attempting to secure a computer system against hostile intrusions.

At the beginning of each exercise, students review a scientific article on the topic at hand. They write a short essay on the subject and answer preliminary questions to gain familiarity with the topic and scientific writing. Then, they follow detailed instructions to execute the attack or system protection technique they are studying to gain hands-on experience. Finally, they write a report on the exercise.

Our intention is to provide distance students with a network security training environment and test bed. The environment enables testing and experimentation of crucial and illegal experiments in a safe and isolated environment. According to the results, we have succeeded rather well.

II. Related Work

Topham et al. divide teaching and learning laboratories roughly into three categories [1]: 1) physical laboratories, 2) simulation laboratories, and 3) virtual laboratories. In this section, we briefly present the cyber security laboratories belonging to each category.

A. Physical laboratories

Physical laboratories typically do not offer resource sharing or virtualization. Their reconfiguration time is limited and expensive, and they do not offer any remote access. For example, Liu et al. [2] describe in their work an experiment for teaching management of a computer network laboratory. Their construction consists of a number of physical network devices and computers. In their laboratory, the computers have both MS Windows and Linux installed. Liu et al. [2] divide their experiments into 13 parts covering a number of layers of the OSI model. According to Liu et al. the experiments were helpful to students' future work. Physical devices, however, restrict flexible reconstruction of the laboratory.

B. Simulation laboratories

In simulation laboratories, resources are partially shareable and have application-based virtualization [3]. Application-level reconfiguration offers relatively easy and inexpensive reconfiguration.

DeLooze et al. [4] represent a simulation laboratory in their work. The Virtual Network Simulation (VNS) models

computer networks and network components such as hosts, firewalls, routers, and switches. A simulated network is displayed graphically, showing the current state using icons and colors [4]. Components of the systems are the Internet Attack Simulator (IAS) and one or more Network Simulators (NSs). The IAS provides an onboard library to simulate different kinds of cyber attacks. Lecture modules of offered courses varied from an introduction to hacker methodology to a lesson on deception attacks. As a result, DeLooze et al. reported a significant increase in knowledge level when students participated in practical exercises with simulation support.

The Linux Network Simulator (LiNeS) is a Linux-based network training environment presented by Tateiwa et al. [5]. Users may use a number of virtual network components such as servers, clients, and switching components. LiNeS was developed to educate students on core skills in network administration. These skills include LAN construction, relation between LAN construction and TCP/IP , troubleshooting, and network security.

C. Virtual laboratories

Virtual laboratories can be divided into several categories according their properties [3]. They typically offer diverse possibilities for resource sharing and reconfiguration. Virtualization type can vary from application-based constructions to multiple virtual machines.

Maleh et al. [6] represent a virtual machine laboratory for education in network security. The Virtual Cloud Lab (VLC) consists of a number of components: 1) a web-based end user interface, 2) a resource manager (VLC), 3) a repository of images, 4) computer hardware, storage, and networking, and 5) security components [6]. Users log in to a remote VLC main page, reserve resources, and select a calculation environment. The corresponding image is executed on a computer.

Xu et al. [3] introduce a cloud-based virtual laboratory in their work [3]. The system consists of a cloud server system, an HP OpenFlow switch, an array of iSCSI Storage Area Networks (SANs), and a Uninterruptible Power Supply (UPS) system [3]. Users log in to the system using the front-end web portal. Once instructors have configured experiments, they are submitted to the back-end Virtual Resource (VR) engine. According Xu et al. [3], the pedagogical model of their experiment can be divided into three phases: 1) knowledge transfer, 2) practice, and 3) knowledge creation. Xu et al. reported improved grades and an increased percentage of students finishing experiments.

III. Interactive Network Security Training Environment

VirtualBox is a powerful virtualization environment freely available as open source software [7]. VirtualBox can be installed on Windows, Linux, Macintosh, and Solaris hosts and supports a number of guest operating systems. Our construction consists of a VirtualBox environment and a number of virtual computers installed on it: Gateway, DNS/DHCP -server, web server, attacker, and a number of clients. A possible system architecture of the construction is presented in Fig 1.

The host machine is typically a Ubuntu-based laptop or desktop. At the beginning of the experiment, an instance of VirtualBox is installed on the host. Virtual guest machines are installed on the host using VirtualBox's tools and ISO image downloads. We used ubuntu-14.04.4-desktop-amd64.iso, ubuntu-14.04.5-server-amd64.iso, and kali-linux-2017.3-amd64.iso images.

The first phase of the work consists of installation and configuration of the gateway. This is a connection point to the Internet and two internal virtual subnetworks, 192.168.1.X and 192.168.2.X. Appropriate modifications must be made to the /etc/network/interfaces file. After that, a simple firewall is implemented using the iptables tool.

A DNS/DHCP server is installed and connected to the virtual subnetwork 192.168.1.X. An instance of bind9 is installed on the server; bind9 is a widely used domain name server in Linux-based systems. Then, a dynamic host configuration protocol server (isc-dhcp-server) is installed. Installation and configuration of the DNS/DHCP server is time consuming and requires caution. Gateway and DNS/DHCP servers are installed using a server image.

The web server is installed using a desktop image and connected to the virtual subnetwork 192.168.2.X. An instance of LAMP server is installed on the web server. The LAMP server consists of the Linux operating system, the Apache HTTP server, the MySQL RDBMS, and the PHP/Perl/Python programming language. After installation and configuration, a number of clients and attackers are installed using desktop and/or kali images.

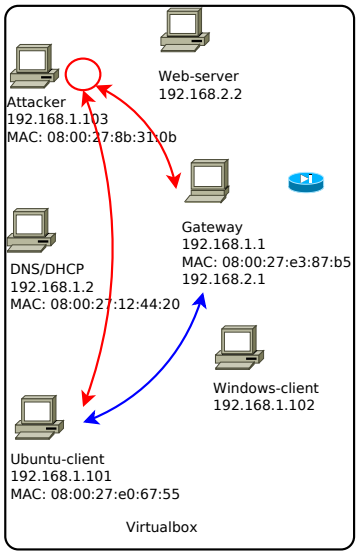

Fig. 1. Simulation Laboratory architecture presenting ARP poisoning.

In comparison with the categories of teaching and learning laboratories, our implementations mostly belong to the category of simulation laboratories. Students download components and install a virtual system on a laptop or desktop of their own. The implementation consists of a couple of physical exercises as well, namely system penetration using Kali Linux and Wi-Fi Protected Access (WPA) dictionary attack.

One of the objectives was to provide students with experience in installation and configuration of Linux-based systems, which is why we did not use cloud-based distribution and/or installation. Installing a virtual system on students' own machines enables a full range of experiments.

IV. Subject Matters and Pedagogical Considerations

The objectives of our work are to provide students with experience in installation, configuration, and administration of a computer system, an interactive network security training environment, experience with cyber attacks in a safe environment, and knowledge of how to protect a computer system against a hostile intruder. The objectives of our work and teaching topics in 2018 are presented in Table I

TABLE I
Pedagogical objectives for CSL education in 2018

Objective		Topics
Installation and administration	1	Installing virtual environment and virtual computers
Cyber attacks	2	System penetration using Kali Linux
	3	WPA dictionary attack
	4	ARP poisoning and ICMP redirecting
	5	DNS and DHCP spoofing
	6	Annoying HTTP server and bank attack
	7	Cracking HTTP pages
	8	Various penetration tests
	9	Reverse TCP attack
System protection	10	Configuring VPN connection
	11	Public key encryption using GPG
	12	Configuring pfsense and snort
	13	Intrusion detection

Installation and administration focuses on installing the VirtualBox environment and a number of virtual servers and computers. Students learn to install and configure a gateway, a DNS/DHCP server, and a web server including a LAMP server. The gateway offers access to the Internet and the services of a firewall. Additionally, students install a number of virtual computers and an attacker. Detailed instructions are given to the students.

Cyber attacks consist of a number of exercises on hostile intrusion and cracking techniques. Experiments vary from penetration tests to ARP poisoning and ICMP redirection. Initially, topics 2 and 7 were as follows: 2) Cracking WEB protocol using aircrack and 7) Downgrading Secure Shell (SSH) protocol. However, WEB protocol is no longer used because of its vulnerabilities, and SSH downgrading is prevented in present versions. Therefore, these topics are replaced by those presented in Table I.

System protection focuses on protecting computer systems from attempts of hostile intrusions. Experiments consist of configuring a Virtual Private Network (VPN) connection, public key encryption using Gnu Privacy Guard (GPG), configuring a firewall, and preparing an intrusion detection system.

Let us consider, for example, exercise ARP poisoning and ICMP redirecting. The ARP is typically used for discovering Medium Access Control (MAC) addresses associated with IPv4 addresses. In ARP poisoning, the attacker sends spoofed ARP answer datagrams to the victim in order to poison its ARP cache. Figure 1 presents an example of ARP poisoning. Initially, the output of the ARP cache of an Ubuntu client may look like

```
dnsdhcp.chydenius.fi (192.168.1.2) at
  08:00:27:12:44:20 [ether] on eth0
gw.chydenius.fi (192.168.1.1) at
  08:00:27:8b:31:0b [ether] on eth0
```

and all the traffic destined to the gateway goes to the attacker. Students perform the same kinds of experiments and report their results.

A number of teaching lessons are given at the beginning of the course. Lessons provide some preliminary knowledge on the topics. They are given in face-to-face sessions and recorded on a Software as a Service (SaaS) cloud service [8]. Students may follow lessons either face-to-face from a distance or by watching on-demand videos from the cloud service [9]. An objective of the course is to give students hands-on experience in the administration of computer systems and on network security training in a hostile computer environment. That is why the role of lessons taught by the educator have less importance than the simulated experiments.

Material is distributed using an electronic Learning Management System (LMS). The workspace used at the LMS consists of a front page and pages for lecture notes, studying the LaTex typesetting system, exercises, background articles, return boxes, contact information of the educator, and a message board for interaction.

Every experiment consists of preliminary questions based on scientific articles, detailed instructed exercises, and a number of questions on the relevant topic. Students prepare reports and return them to the learning environment. The instructor evaluates the reports and gives the final scores.

V. Results and Discussion

This study is the first step in an iterative process aimed at developing The Network Security course. In this stage of development, the experiences of students and teachers from the current implementation of the course have been collected. Based on this information, the following development steps can be designed.

The curriculum was organized three times, in 2015, 2016, and 2018. We had a total of 33 enrolled students, of which 26 successfully passed the course. Statistics of accomplishments are presented in Table II.

TABLE II
STATISTICS OF ACCOMPLISHMENTS AT THE CURRICULUM.

	Enrolled	Bypassed
2015	13	7
2016	11	10
2018	9	9

As can be seen from the Table II, seven students succeeded in passing the course in 2015 and five dropped out. According to these statistics, four out of five students who dropped out did not succeed in installing and configuring the system. The last dropout in 2015 and the dropout in 2016 gave up after experiment number 2. We assume that students considered the experiment of installation and administration rather time consuming and burdensome. In 2018, however, all active students successfully passed the course. One of the reasons for this, we assume, is that we translated the instructions from English to Finnish.

Review was based on resolved experiments and correctness of reports. The number of credit points was based on number of experiments passed: 9 out of 13 earned 3 ECTS, 11 out of 13 earned 4 ECTS, and 13 out of 13 earned 5 ECTS. Exercise questions were primarily formulated to help students succeed in passing the exercise and understanding the basic ideas of the experiment . Except for the experiment of installation, we do not see a tendency of one exercise being more difficult than another.

Students are asked to evaluate the setup of the curriculum in their own words: what was interesting in the exercise, what kind of difficulties they had, and so forth. Answers were asked after each experiment, and a total of 294 answers were collected. According to textual analysis, four main topics were noticed. Students noticed that the experiments 1) were interesting, 2) motivated them, 3) gave them a reasonable challenge, and 4) were educational.

Most of the students considered the experiments interesting. That was because they accomplished hands-on experiments in addition to learning theoretical elements. Those hands-on elements were motivating as well.

The experiments were quite challenging, especially for those who had less experience in administration. Problems mostly arose as a result of carelessness in writing specification files of Linux. Some other problems arose as a result of lack of documentation and some outdated commands.The students considered the experiments educational. According to one student, the best way to defend against an attack is learning to perform attacks.

Our study program typically offers lecture type education by prerecorded transcriptions. Considering viewing statistics of implementations, we noticed that preparatory type lectures and prerecorded transcriptions were necessary and accompanied. Guidance type transcriptions did not obtain popularity.

As a result, students considered installation and system administration experiments rather demanding. Therefore, this could be a voluntary module. The other experiments could be divided into a number of separate modules so that students are able to accomplish them on a cloud-based virtual environment.

VI. CONCLUSIONS AND FUTURE WORK

This paper has presented an experiment of an interactive network security training environment. The training environment provides students with experiences in installation and administration of a computer system, training their skills in network security and in protecting a computer system in a hostile environment. The environment consists of a number of introductory lessons, an LMS system to distribute material, a simulation environment, and a number of experiments on relevant topics. As a result, we can conclude that the environment has been encouraging and assisted students in their self-studies. Feedback from students has been supportive and mostly positive. Students considered the experiments demanding and laborious but interesting.

VII. ACKNOWLEDGEMENTS

The idea of the work and original material was provided by Secure Communications Engineering and Signal Processing group (SCSP) at the University of Jyväskylä. We are grateful for the help.

REFERENCES

[1] L. Topham, K. Kifayat, Y. Younis, Q. Shi, and B. Askwith, "Teaching and learning laboratories: A survey," *Information & Security: An International Journal*, vol. 35, pp. 51 – 80, 2016.

[2] Y. Liu, L. Zhang, and F. Jiao, "Teaching computer networking experiment in the realistic network laboratory," in *Proceedings of International Conference on Computational Intelligence and Software Engineering*, 2009, pp. 1 – 4.

[3] L. Xu, D. Huang, and W. Tsai, "Cloud-based virtual laboratory for network security education," *IEEE Transactions on Education*, vol. 57, no. 3, August 2014.

[4] L. DeLooze, P. McKean, J. Mostow, and C. Graig, "Incorporating simulation into the computer security classroom," in *Proceedings of 34th Annual Frontiers in Education*, vol. 3, 2004, pp. S1F/13 – S1F/18.

[5] Y. Tateiwa, K. Kurachi, J. Zhang, T. Yasuda, and S. Yokoi, "LiNeS: Virtual network environment for network administrator education," in *Proceedings of 3^{r}d International Conference on Innovative Computing Information and Control*, Dalian, Liaoning, China, 2008, pp. 1 – 4.

[6] Y. Maleh, A. Sahid, A. Ezzati, and M. Belaissaoui, "Building open virtual cloud lab for advanced education in networks and security," in *Proceedings of International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2017, pp. 1 – 6.

[7] Oracle, "Welcome to virtualbox.org!" https://www.virtualbox.org/, refered June 8, 2019.