Available online at www.sciencedirect.com

ScienceDirect

Procedia - Social and Behavioral Sciences 141 (2014) 10 – 14

Procedia
Social and Behavioral Sciences

WCLTA 2013

Applying Virtualization Technology in Security Education

Wenjuan Xu [a] *, Kevin Madison [b], Michael Flinn [c], Willson Kwok [d]

[abcd] *Frostburg State University, Frostburg 21532, USA*

Abstract

This paper describes how to use the network virtualization technology to facilitate the teaching of different security courses. We introduce how to build and play a virtual network with virtual machines or using the network virtualization supported by the cloud computing. We present and compare the results of using these two different kinds of technology in security courses from aspects such as acceptance, convenience, cost, performance and security.

Selection and peer-review under responsibility of the Organizing Committee of WCLTA 2013.

Keywords:

Main text

Experiential learning is very important for a student to understand different course concepts. In the security education, to better understand security theories, students often need to have access to sophisticated security tools as well as the capability to install and configure related applications. For example, to understand how a penetration testing is performed in an ethical hacking course, students need to identify vulnerable systems in the network and perform hacking with different hacking tools. This means in some settings, the students need to expose to the whole network infrastructure as well as the tools used by attackers to compromise the security of the system. These activities are something that the university network administrator works hard to prevent. Also, if the students want to perform a task as such as a denial of service attack with several machines to work together, machine supplies is a challenge for the university lab environment.

* Corresponding Author: Wenjuan Xu. Tel.: 001-301-687-4042
E-mail address: wxu@frostburg.edu

Selection and peer-review under responsibility of the Organizing Committee of WCLTA 2013.
doi:10.1016/j.sbspro.2014.05.004

To solve these challenges, virtualization technologies are introduced in different works. The work by Tim [1] explains how they use different virtualization technologies in education. Dale [2] describes their experience in applying virtualization technologies in information systems education. IBM [3] explains applying virtualization technologies into the education. With the virtualization [4], you can run different operating systems and applications on a single computer. Also you can obtain better host security since the virtual machine running in a relatively isolated environment. In addition, virtualization has features such as saving computer work status and easy managing hardware etc. These features offer similar benefits in security education. Using virtualization technologies, a student can configure several virtual machines to compose an isolated network infrastructure using only one work station. Also, if there is any malicious software installed or hacking performed, the host computer has high possibility to stay in security. In addition, virtualization enables a student keeping the status of their work as saved and he can come back to work on it or even allows the student engaging in projects build on one another. In case there are applications having higher hardware requirement, the students can easily manage the virtual machine to satisfy that.

Other than the traditional virtualization technologies discussed above, cloud computing [5] technology has been the most discussing topic in industry and academic. As defined by Gartner [6], "Cloud computing is a style of computing where scalable and elastic IT enabled capabilities are delivered as a service to external customers using Internet technologies". This means that if people want to access a public cloud service, the only thing they need is the internet and browser. There are different cloud computing service providers such as Amazon AWS [7], HP Cloud [8], Google Cloud [9], Microsoft Cloud [10], and IBM Cloud [11] and so on. Different service providers have different focuses and features. In this paper, we select one of the top cloud provider Amazon AWS as the example. Amazon AWS [12] is a cloud computing service supporting database, storage, networking, management and different application service. For example, a student can use AWS networking service to build a virtual network similar as traditional virtualization technologies. Also AWS provides additional features such as global access, strong authentication mechanisms, storage and database supporting etc. Investigating how these features can benefit the security education will be meaningful.

The paper will describe and compare how the students apply the traditional virtualization technology and the cloud computing into two example security courses-the network security course and the ethical hacking course. The paper has four sections. The first section introduces this paper. In the second section, we will describe how to build virtual network environments with the traditional network virtualization technology and the cloud computing. Third section introduces how we apply the two different network technologies into the example security courses and compare the results based on the student's feedback. In the last section, we summarize our work.

1. Virtual Technologies for Building Virtual Networks

The network architecture can be generally classified into client-server based and peer to peer based [13]. In the following, we will explain how to build the two different network architectures with the traditional virtualization and the cloud computing. We will also describe what kind of features supported by the two technologies.

2.1 Traditional network virtualization technology

2.1.1 Building virtual networks with traditional technology

Currently, VMware Player [15] and VirtualBox [16] are two main free, desktop applications for running a virtual machine. They have the similar features as follows. (1)The virtual disk drive of the virtual machine is an image file of a drive containing different operating systems. (3) Supporting network adapters include Bridge, NAT and Internal. With a configured a Bridge adapter, the virtual machine can communicate with the host computer. Configured with a NAT adapter, the virtual machine can access the internet through the host computer. Several