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.

© 2014 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/3.0/).
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
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
virtual machines can compose an isolated network through configuring them with the internal adapters. (4) The virtual machine can access host computer devices such as the removable USB drives and shared folders. (5) In the VMware Player and Virtual Box, the user can view, configure, start and stop the virtual machine.

To build an isolated client-server network with virtual machines, we need at least two parties including the server side and the client side. To be in the same network, the server and the client virtual machines should all be configured with an internal network adapter. Then we can assign static IP address or dynamic IP address for the machines as the normal client-server network. We can also add more server or client virtual machines into the virtual network with the similar network configuration. In addition, if a server needs to be publicly accessible, a bridge network adapter is required for the server virtual machine. Through bridging this server out, the IP address of the server is accessible by other host computers.

Similar with the client-server virtual network, we can build a P2P network through having several virtual machines running on the host computer. Each virtual machine is configured with two network adapters including NAT and Internal. With the similar IP address assigning as a normal P2P network, a virtual P2P network is composed in which virtual machines can access to the internet and communicate with each other.

2.1.2 Security features

The virtualization provides a relatively isolated environment through encapsulating everything of the virtual machine. The user of the virtual machine can be super user or common user depending on the set up. The super user can install the different software without endangering the security of the host computer. In case the virtual machine is impaired, the student can recover that with the backed up image. However, due to the huge size of the virtual machine file, it is inconvenient for the students to move their virtual machine to other host computers. In addition, the virtual machine can share folders, USB and devices, which bring potential security issues.

2.2 Cloud computing network virtualization technologies

Amazon AWS is a comprehensive cloud service platform that offers the service supporting for the database, storage, and network. In the network service, Elastic Compute Cloud (EC2) and Virtual Private Computing (VPC) are mainly used for building various virtual networks. Rather than explaining everything of AWS, in the following, we describe how to build different virtual networks using EC2 and VPC.

2.2.1 Building a virtual server network with EC2

To use the EC2, the user first needs to build different instances (virtual machine) and then work with the instances. To build an instance in the EC2, students need several steps as follows. (1) Sign in to the AWS accounts. (2) Select the EC2 service and click the Launch Instance button to begin. (3) Select the operating system such as windows server 2008R2, Ubuntu 12.04.2 LTS. (4) Set up monitoring and shutdown behaviour for the instance. (5) Create a unique key name for the built instance. (6) Configure a key pair for the built instance. In the EC2 management console the user can configure, view, start and stop the instances. To remote into an instance built, the user needs to select the instance intended to start, input the username and password based on the key pair built before, and the EC2 instance will start to work. The user can then work in the EC2 instance. For example, the user may enable the web server service in the EC2 instance. Later, different users in the world can access this web server with the public IP address of the EC2 instance.

2.2.2 Building a virtual network with VPC
The VPC supports the user to build an isolated client-server network or P2P network. In this network, the user can specify a reasonable private IP address range, divide the chosen IP addresses into one or more public or private subnets, and have control over inbound and outbound access to and from individual subnets. Data stored in Amazon’s database service can have permissions set to only allow access from the user’s VPC. The user can assign multiple IP addresses to his VPC along with attaching multiple network interfaces. Attach one or more Amazon elastic IP addresses to any instance in the VPC so it can be reached directly from the Internet.

To set up a VPC, the user needs to start the VPC and then build the instances into the VPC. To start the VPC, there are three main steps. (1) Click the “start VPC wizard” (2) Choose the VPC type with the choices -- a single public subnet only, with public and private subnets, with public and private subnets and hardware VPC access, and with a private subnet only and hardware VPN access. (3) Review the settings for the VPC and create the VPC. To build and work on the instances in the VPC, users need to follow the similar steps in EC2.

2.2.3 Amazon AWS Security Features

To provide strong user’s authentication, AWS supports mechanisms such as access credentials, sign-in credentials, key rotation, PGP and so on. Other than the credentials, the instance OS created in AWS is isolated from the host computer. Different with the traditional virtual machine technology, we cannot share device and folder between the AWS instance and the host computer.

2. Apply Virtual Technologies into Security Education

Most of the network security courses need a virtual environment to complete varied assignments. In the following, we explain our experience about using the traditional virtual network and cloud computing in the network security course and the ethical hacking and defence course with sample projects.

3.1 Network security course

In this course, students are required to build an isolated client-server network configured with DNS server, DHCP server and directory server for managing several client computers. Web server and email server are also installed in this network. Servers and clients should be implemented with a list of security methods such as installing firewall, enabling anti-virus and so on.

3.2 Ethical hacking and defence course

In this course, students are supposed to have an isolated P2P network, in which several computers are working as the attacker and several computers are the target. Sample projects include performing such as the denial of service attack, user name and password attack, information intercepting and so on. Students are required to install different malicious and security software on the attacker machines and the target machines.

3.3 Comparison

Students can finish the assigned projects for the two courses with both virtualization technologies. Based on the feedback and observation collected, the follows are the comparison results.

- **Acceptance:** At the beginning, students prefer to use the traditional virtual technology which they are more familiar with. However, after students learn how to use the EC2 and the VPC, they can accept that.
Convenience: Students prefer the cloud computing from the convenience aspects due to two reasons. (a). Global reach supporting students their work with any computers. (b). Database and storage supporting provides students more flexibility when they need to back up their information and virtual images.

Cost: The using of the traditional virtual technology is free. Students complain about the charging for using AWS service such as uploading and downloading resource and help desk services.

Performance: For the AWS service, every instance is running in the cloud and the host computer is only for remote accessing. When there are requirements of several virtual machines running at the same time, the AWS service is preferred in the performance aspects. If only two or one virtual machine is required, students prefer the traditional technology since it does not need to worry about the remote access.

Security: There are some students concerning about the resource sharing feature in the traditional virtual technology.

3. Discussion and Summary

In this paper, we first explain how to build different virtual networks with the traditional virtual technology. Second, we use Amazon AWS as the example cloud service to describe how to implement different kinds of virtual networks, and what kind of security features that AWS can provide. Then we separately apply the traditional virtual technology and cloud computing into the two security courses. Based on the feedback and observations of the students, we compare and summary the results. In the future, we will investigate other virtual network technologies to help the students for the experience learning in the security courses.

References


Michael Armbrust & Armando Fox & Rean Griffith etc.(2009), EECS Department, University of California, Berkeley.


Virtual Box. Available on: https://www.virtualbox.org/