Work in Progress - Improving Web Security Education with Virtual Labs and Shared Course Modules

Lixin Tao, Li-Chiou Chen, and Chienting Lin
Pace University, ltao@pace.edu, lchen@pace.edu, clin@pace.edu

Abstract - **One challenge in web security education is its interdisciplinary and practical nature. Students need to have the basic knowledge and skills of a web developer to understand many of the web security topics, and some of them are normally covered in multiple advanced courses like Computer Networks and Network Security, or are absent from many existing undergraduate or graduate degree programs. This paper shares our experience of using VMware virtual machines in supporting hands-on web security education, and developing multiple virtual web security lab modules based on the virtual machines. The lab modules are part of our NSF SWEET (Secure WEb dEvelopment Teaching) project, and each of them contains (1) concepts in a nutshell; (2) lab objectives; (3) software setup; (4) detailed lab instructions; and (5) lab evaluations. Comprehensive lab modules have been developed to guide students to build virtual Ubuntu virtual machines with publicly available tools and install all necessary web servers, application servers and database servers on them so they can function as the foundation and platforms of the other course modules. The other covered course modules include cryptography, HTTP and HTTPS protocols, and introduction to Java web technologies.**

Index Terms - Network security, Virtual labs, Web technology, Web security.

INTRODUCTION

One challenge in web security education is its interdisciplinary and practical nature. Students need to have the basic knowledge and skills of a web developer to understand many of the web security topics, and some of them are normally covered in multiple advanced courses like *Computer Networks* and *Network Security*, or are absent from many existing undergraduate or graduate degree programs (like Ajax or web services). The students also need to actually practice to learn how to prevent, identify and resolve web security breaches, but limited university resources and few local web security domain experts sometimes limit the scope and scale of projects that students could practice in lab environments. If such labs are not designed properly, students could also cause web security problems when they explore security vulnerabilities of university or company public web sites.

This paper shares our experience of using VMware virtual machines in supporting hands-on web security education, and developing multiple virtual web security lab modules based on the virtual machines. The lab modules are part of our NSF SWEET (Secure WEb dEvelopment Teaching) project, and each of them contains (1) concepts in a nutshell; (2) lab objectives; (3) software setup; (4) detailed lab instructions; and (5) lab evaluations. Comprehensive lab modules have been developed to guide students to build virtual *Ubuntu* virtual machines with publicly available tools and install all necessary web servers, application servers and database servers on them so they can function as the foundation and platforms of the other course modules. The other covered course modules include cryptography, HTTP and HTTPS protocols, and introduction to Java web technologies. All the lab modules can be installed on portable USB thumbnail disks and run on any computer that installs the free VMware Player. The paper will also present our experience in adopting these course modules in multiple network and web security courses at Pace University.

SELECTION OF COMPUTER LAB VIRTUALIZATION TECHNOLOGIES

The virtualization of a computer means to run emulator software, like VMware Player [1] or Microsoft Virtual PC [2], on a computer (host computer or physical computer) to emulate another desired computer (virtual computer). There are two virtualization technologies: (1) server-side virtualization for running the virtual computers on a remote server computer, and (2) client-side virtualization for running the virtual computers on users' own computers. While company/university IT infrastructure servers can use the server-side virtualization to improve resource utilization, client-side virtualization greatly reduces the pressure on the servers and network bandwidth, and take advantage of faculty and student PCs' excessive computing power already available today. In the recent years we have studied many PC/lab outsourcing services based on server-side virtualization and concluded that they all have recurring high costs or very limited flexibility and resources for the users.

The main advantages of client-side computer virtualization for university computer labs include (1) no cost for specialized hardware; (2) the complete lab environment could be set up on the VMs (virtual machines)

978-1-4244-6262-9/10/$26.00 ©2010 IEEE

by the instructors and distributed to the students as file folders; (3) the students can run the VM and work on the customized labs on any computer that has installed a small and open source VM player; (4) the students can install new software and modify the exiting installation.

For our web security virtual labs we choose VMware virtualization over Microsoft Virtual PC because the former can support virtual machines running any operating system including all flavors of Linux.

UBUNTU SECURITY LAB PLATFORM

A complete lab module has been developed for students and faculty who have no Linux background to develop a Ubuntu v9.10 (the latest version) virtual machine (VM). Instructions are also included to install and configure most necessary IT servers and tools needed for supporting network/web security and computing technologies. The tutorial module includes (1) a detailed lab manual "A Tutorial on Setting up Ubuntu Linux Virtual Machines" [3] detailing step-by-step guidance to achieve the above tasks; (2) 7z auto-extracting file for the completed basic Ubuntu v9.10 VM ready for software installation [4]; (3) 7z auto-extracting file for the completed Ubuntu v9.10 VM ready for lab use or distribution to the students [5]; and (4) a video tutorial for those who need further visual help[6].

Among the others the VM ubuntu10 supports (1) Tomcat web server v6.0.20, (2) Apache web server v2.2 with support for Perl, PHP and MySQL; (3) MySQL database server v5.1; (4) Eclipse IDE v1.2.1 (Galileo SR1); (5) NetBeans IDE v6.7.1; (6) GlassFish application server v2.1 including Java EE web server); and (7) Drupal web contents management system v6.14

SECURITY LAB MODULE ON CRYPTOGRAPHY

Security lab module "Introduction to Cryptography" [7] covers fundamental concepts of symmetric secret key ciphers, public key ciphers, hash functions, digital signatures and digital certificates. The lab has the following objectives:

a. Learn and practice how to use MD5 and SHA1 to generate hash codes of strings or large files, and verify whether a downloaded file is valid;
b. Learn and practice how to use GPG to encrypt/decrypt files with symmetric algorithms;
c. Learn and practice how to use GPG to generate public/private key pairs and certificates, distribute the certificate with public key to a friend, let the friend encrypt a document with the public key, and let the key owner decrypt the document with the private key.

As our other lab modules, this module also has a rich set of evaluation questions to check how well the students have understood the essence of the lab module, and guide them to creatively apply the learned concepts and skills in solving related questions.

SECURITY LAB MODULE ON WEB TECHNOLOGIES

Security lab module for introducing web technologies [8] covers the web architecture, uniform resource locators, HTML basics, the HTTP protocol, web session data management (cookies, hidden fields, query strings and server-side session objects). The lab has the following objectives:

a. Compare HTTP GET and HTTP POST requests;
b. Observe HTTP communications with proxy server Paros;
c. Experiment with cookies through web applications;
d. Compare web browser and web server interactions with HTML forms and with hyperlinks;
e. Learn how to use JavaScript to validate form data in the web browsers;
f. Learn how to create a static web site;
g. Learn how to create your first JSP web application on Tomcat;
h. Learn how to create your first servlet web application on Tomcat.

The lab has the following sub-sessions:

1) Comparing HTTP GET and HTTP POST Requests
2) Observing HTTP Communications with Paros
3) Working with Cookies
4) Submitting Data with HTML Form and Hyperlink
5) Validating Form Data with JavaScript
6) Creating Your First JavaServer Page Web Application
7) Creating Your First Servlet Web Application

WEB SECURITY LABS ADOPTION EXPERIENCE

Most of our web security lab modules have been successfully incorporated in the undergraduate course "Overview of Computer Security" and graduate courses "Web and Internet Security" and "Concepts and Structures of Internet Computing". We collected students' feedback on the SWEET modules adopted in two classes of "Overview of Computer Security" and "Web and Internet Security" offered in Fall 2009. A web-based survey using 5-point Likert scale was conducted at the end of the semester. The survey included questions to elicit their feedback on the lecture materials, laboratory exercises, the mapping between the lecture and the lab and the overall impact of these modules on their learning. Our results show that the students had invested significant amount of time (2-4 hours per week on average) in completing hands-on exercises. However, they generally agreed that the course materials were planned well (average 4.1 for lecture category), the exercises had drawn their interests (average 4.1 for lab exercise category), the exercises had helped them in learning the course materials (average 4.1 for the mapping between labs and lecture), and they would be interested in pursuing further in

the Information Assurance area (average 3.9 for overall category).

ACKNOWLEDGEMENT

This work was supported by the NSF CCLI 0837549. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the National Science Foundation or the U.S. government.

REFERENCES

[1] VMware Inc., "VMware Player", http://www.vmware.com/products/player

[2] Microsoft Inc., "Microsoft Virtual PC", http://www.microsoft.com/windows/downloads/virtualpc

[3] Tao, L, "A Tutorial on Setting up Ubuntu Linux Virtual machines", http://csis.pace.edu/lixin/ubuntu/LinuxTutorial.pdf, 2010

[4] Tao, L, "ubuntu10basic.exe", http://csis.pace.edu/lixin/ubuntu/ubuntu10basic.exe, 2010

[5] Tao, L, "ubuntu10.exe", http://csis.pace.edu/lixin/ubuntu/ubuntu10.exe, 2010

[6] Tao, L, "A Video Tutorial on Setting up Ubuntu Linux Virtual machines", http://csis.pace.edu/lixin/ubuntu904, 2009

[7] Tao, L, "Introduction to Cryptography", http://csis.pace.edu/lixin/download/lab-cryptography.pdf, 2010

[8] Tao, L, "Introduction to Web Technologies", http://csis.pace.edu/lixin/download/lab-introduce-web.pdf, 2010