Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

Virtual Lab for Information Assurance Education

Azene Zenebe and David Anyiwo
Department of Management Information Systems, Bowie State University

Abstract - The need for skilled information assurance (IA) professional requires educational programs that impart both theoretical knowledge and practical skills through hands-on lab activities. Students need to develop skills by conducting security related experiments or hands-on lab activities in safe and isolated systems and networks environment. Furthermore, more and more information technology (IT) professionals who want to earn graduate level training in IA are likely to be enrolled in online programs and classes. Hence, providing remote access to labs becomes a necessity for this population of students. This paper presents our approach to provide remote access to laboratories, which are accessible by any student and faculty who has Internet from anywhere 24/7, for students and faculty so that they can develop skills that are readily applicable in the workplace. Furthermore, the paper presents the virtualization technology used, challenges, and several hands-on lab activities that are performed by students in information systems graduate courses.

Index terms – virtual lab, information assurance, online education

I. INTRODUCTION

The continuous and pervasive growth of information systems in every area of human endeavor has significantly increased the threats to networks and to information contained in databases or repositories. Security issues have become commonplace in information systems, making familiar such terms as hacker attacks, malicious code, viruses, worms, Trojan horses, cyber-espionage, and disaster recovery. The professionals in charge of preventing, analyzing and counter-attacking these threats are known as information assurance professional, and they need to have the necessary knowledge and skills.

The need for skilled information assurance (IA) professional requires educational programs that complement theory with hands-on experiences. Students need to develop skills by conducting security related experiments or hands-on lab activities in safe and isolated systems and networks environment. Furthermore, more and more IT professionals who want to earn graduate level training in IA are likely to be enrolled in online programs and classes. Hence, providing remote access to labs becomes a necessity for this population of students.

This paper presents our approach to provide remote access to laboratories for students so that they can develop skills that are readily applicable in the workplace. Furthermore, the paper presents the virtualization technology used and several hands-on lab activities that are performed by students in information systems graduate courses.

II. IA CURRICULUM

The graduate program in information assurance (IA) program is designed to prepare students for careers in the analysis, design, implementation, and management of information systems and information technology with focus of Information Assurance. The program requires a minimum of 36 semester hours consisting of three (3) basic, seven (7) core and three (3) electives courses from one of the three concentration tracks: Database and Web Security, Information Assets Protection, and Network Security.

The Maryland Higher Education Commission (MHEC) has awarded a grant to Bowie State University to support the development of this program. The Department of Management Information Systems at Bowie State University, with the technical assistance of the Division of Information Technology, developed the curriculum, the online courses and labs. The program also targets many jobs involved in the base realignment and closure (BRAC) process that deal with information security issues; these are identified as “primary positions” (direct employees of department of defense(DoD)) and “secondary positions” (DoD contractors). The realignment and closure (BRAC) of U.S. military bases across the nation is causing nearly 60,000 jobs to move into Maryland due to the relocation of military personnel, their relatives, and military contractors. Patel and Stephenson [1] analyzed the educational needs of this new contingent of workers, once they move to Maryland. Due to the technical nature of most of the relocated positions, they found that the higher education needs are in the areas of Engineering, Computer Science, and Information Technology (IT).

The IA program will also allow others in the region to enroll in the program and acquire critical knowledge and skills for developing organizational security plan, programs, policies and standards, managing current policies, and analyzing emerging issues in the area of internal and external information threats.

The IA curriculum, designed primarily for online delivery, is aimed at employed adult learners that cannot commute daily to campus, and will provide unique learning experiences through virtual laboratories that mimic the

work environment of IT security professionals. Most IA courses have laboratories that correspond to problems in the workplace.

Generally, laboratory experiences are typically conducted in an isolated computer laboratory where security problems that may occur are unable to affect other computers on campus. As a result, students do not have remote access to existing lab and this limits students' access to the laboratory. Moreover, for online classes, students often cannot physically come to the campus to access the laboratory. One solution to this problem, implemented in this program, is a virtual security laboratory, which is LAN accessible by any student who has Internet access from anywhere 24/7. Students get into the lab using Remote Desktop Connection (RDC). Once authenticated into the lab, students can access any of the computers in the lab and complete their hand-on laboratory exercises and projects.

III. VIRTUAL LAB

In general, categories of hands-on lab activities to be done by students and faculty are software-based, hardware-based, and hybrid of the two. Examples of software-based hands-on lab activities include:

- Explore the vulnerabilities of different network servers including email, DHCP, DNS, and FTP.
- Explore the vulnerabilities of different application servers including SQL and Web servers.
- Security auditing of the computers on the network by using Nmap.
- Network Traffic Analysis using Wireshark.
- Applied cryptography using PGP and other tools.
- Explore host hardening of both Windows and Linux computers by exploring services, managing users and groups, and inspecting various logs on the computers using tools such as MS Base Analyzer.
- To establish and implement password policies, and policies to ensure data confidentiality, data availability, and data integrity.
- Computer forensics using tools such as Autopsy Forensic Browser and Sleuth Kit.

Examples of hardware-based hands-on lab activities include configure and manage a Cisco firewall and router. Examples of hybrid-based hands-on activity include configure sensors and manage an intrusion detection system like *Snort*.

For the information systems courses, hands-on lab activities are predominantly software-based or hybrid category of experiments. Therefore the emphasis of this Lab is to create an environment where software and hybrid experiments can be supported remotely.

Additional requirements for the Lab include a reasonable performance speed and reliability, security- only authorized students to access the lab facilities by strong authentication methods. There is also a need for coordination of accesses to prevent resource conflicts as well as the development of lab support procedures and usage policy. This document provides detailed procedures for each kind of laboratory environment, and remote access procedures, remote desktop protocol configuration and utilization details, and sign-on and sign-off procedures. Finally, there is a need to develop a *Web-based lab portal that provides a* visual depiction of different labs.

A. Lab Implementation

We use the virtualization approach because of its several advantages reported in similar other work, e.g. [2, 3] such as the ability to create standard configurations and easily cloned to create several virtual machines, the ability to take snapshot of virtual machines and later restore them. Furthermore, virtualization provides secure environment and has low cost.

1. Host

At present, a single host is implemented using the following resources:

- Hardware: An IBM Server with 8 Intel Xeon CPUs, each 2.8GHz, 25 GB of RAM
- Storage: 950.50 GB of hard disk
- Software: ESX 4.0.0, vCenter Server and vSphere 4 Enterprise licensed for 2 physical CPU, and vSphere Client.
- Number of NICs: 7

These resources are described as follows[4]:

- The VMware ESX is a virtualization product offered by VMware, Inc. It allows the creation of multiple virtual machines through abstraction of the processor, memory, storage, and networking resources of the physical host.

- The vCenter Server is a service that acts as a central administrator for ESX hosts connected on a network.
- The vSphere Client is the primary method of interaction and acts as a console to operate virtual machines and as an administration interface into the vCenter Server systems and ESX hosts.

The ESX host is installed and configured, as depicted in Figure 1. vSphere Client is used to access and manage the ESX host as shown in Figure 2.

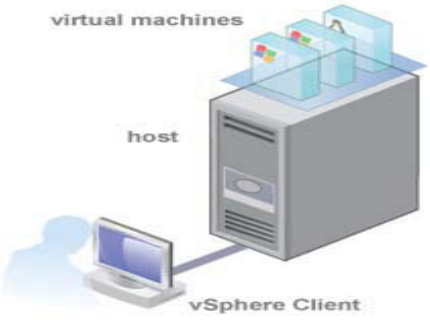

Figure 1. Basic Single-Host Management System (source: [4])

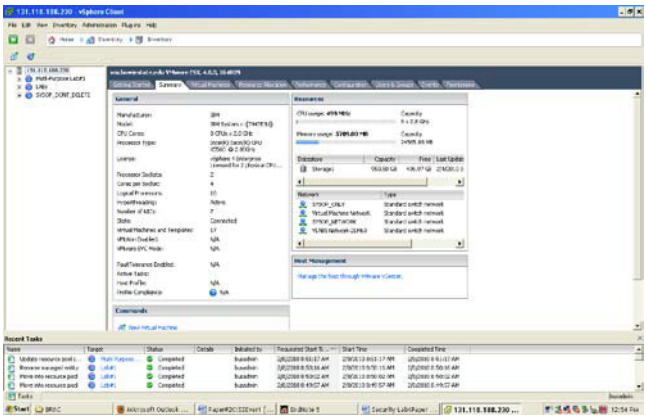

Figure 2. Screenshot for the ESX host while running

After the initial setup of ESX, vSphere 4.0 with vCenter Server will be deployed in order to manage multiple hosts and virtual machines. The architecture is shown in Figure 3; and the vCenter Server uses Microsoft SQL Server 2005 Express for small deployments with up to 5 hosts and 50 virtual machines[4].

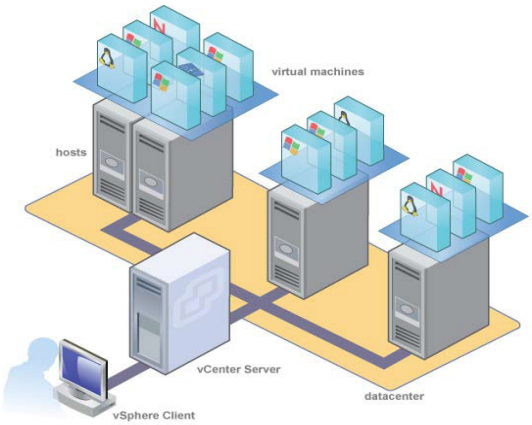

Figure 3. vSphere Components (Source: [4])

2. Virtual Machines

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. Multiple virtual machines can run on the same host at the same time or can also run on a cluster of hosts [4]).

The vSphere Client is used to create and manage virtual machines as shown in Figure 4. There are twelve Windows XP virtual machines, one Windows 7 virtual machine, one Windows Server 2003 virtual machine, one Windows Server 2008 virtual machine, and one Linux virtual machine. These virtual machines are on a standard switch network with 1 Gbps LAN and are connected to the Internet.

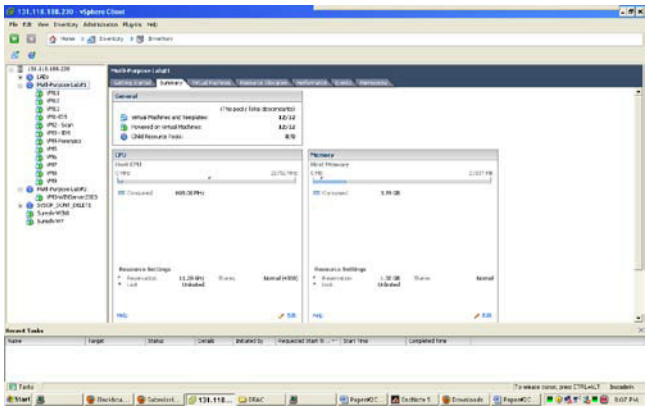

Figure 4. Screenshot for Virtual Machines

Students access these virtual machines and their resources using the remote desktop connection (RDC). Some of the

security tools that are available are Systems Auditing tools such as MS Baseline Security Analyzer and Nessus, network traffic analyzer such as Wireshark, IDS such as Snort, forensics tools such as Autopsy Forensic Browser and Sleuth Kit, and other tools such as Nmap and S-Tool. Whenever necessary, students have administrative access to these virtual machines to install, configure and manage security tools and systems. Oracle 10g DBMS is also available on the Windows Server 2003. A sample screenshots of these virtual machines while in use are presented below in Figure 5 to Figure 10.

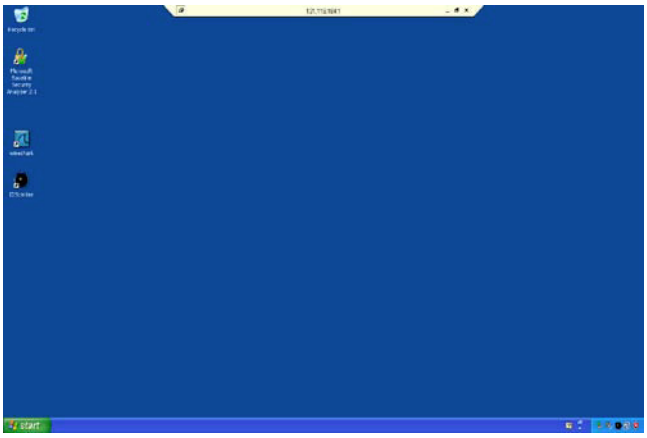

Figure 5. A virtual machine accessed with RDC

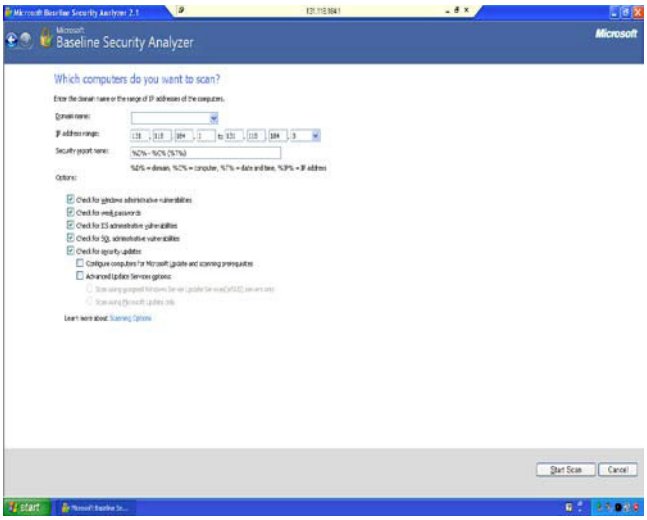

Figure 6. Systems Auditing using MSBSA - Scan Multiple Computers

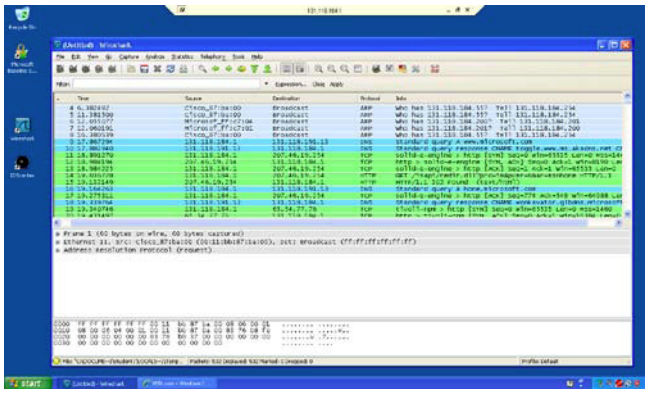

Figure 7. Network Traffic Sniffer and Analyzer

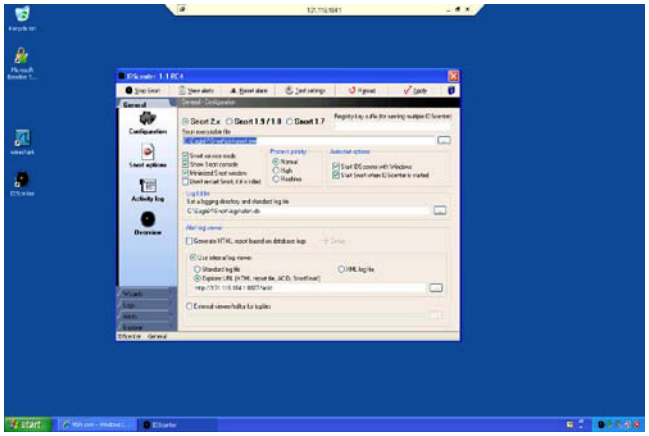

Figure 8. Intrusion Detection with Snort – Setup & Configuration

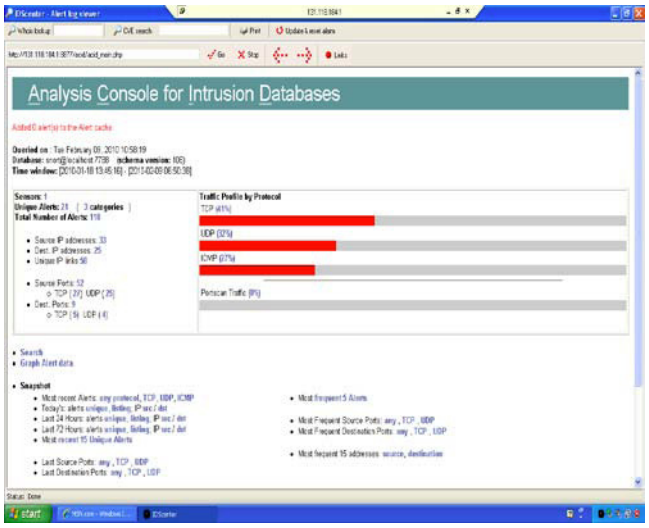

Figure 8. Intrusion Detection with Snort – Output Console

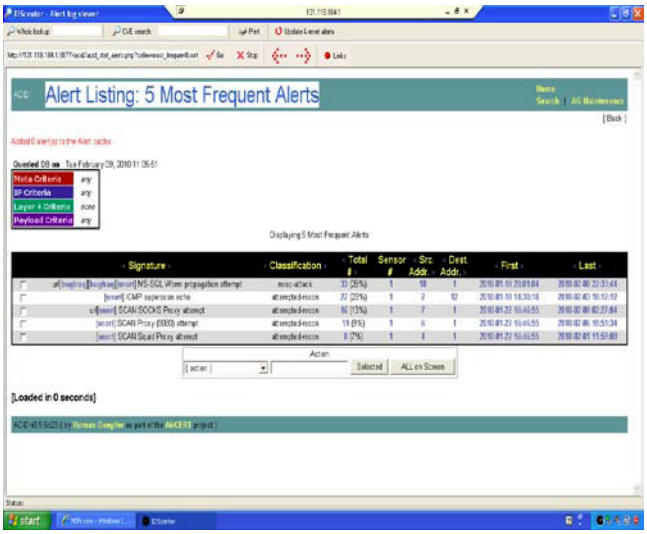

Figure 9. Intrusion Detection with Snort – Alert Listing: 5 Most Frequent Alerts

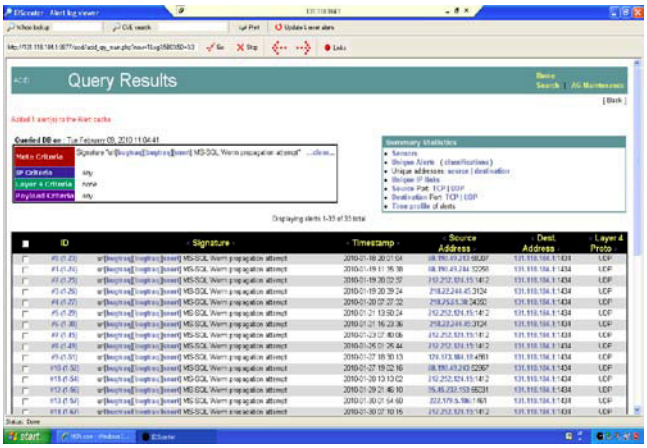

Figure 10. Intrusion Detection with Snort – Example of Alerts: MS-SQL Worm propagation attempt

3. Use of the Virtual Labs

The virtual lab is being used in the Auditing, Monitoring and Detection Intrusion graduate course (INSS 770) in spring 2010. There are 11 students enrolled in the class, and they are expected to complete the following major activities using the VLAB:

a) Project: Students will complete the following tasks:

- Part I: Install, configure and use a Snort IDS.
- Part II: Analyze default Snort rules and write two to four new rules.
- Part III: Students launch intrusion attempts or attacks on other students.
- Part IV: Prepare a report to a manager on detected intrusions for a system monitored by Snort.

b) Hands-on Lab assignments:

- Hands-on Lab #1 – Auditing/Vulnerability Scanning of a client OS, a server OS and a virtual network
- Hands-on Lab#2 – Network Monitoring using Wireshark
- Hands-on Lab #3 – Detection of Trojan Horses

For the project and assignments, each student will prepare a report including answers to questions, their experience in the form of a lab journal and screenshots of the major activities and results. The lab journal reflects on what students are learning in their lab experience based on what they have been doing and seen happening in the lab. We grade both the journals and reports.

Students have accounts to utilize the VLAB. At the end of the semester, we will assess how the added hands-on lab activities affect student learning using pre-test and post-test as well as using opinion survey. By the time of writing this paper, students have completed hands-on Lab #1 assignment and used Wireshark to complete in class exercises. A few students provided the following comments:

- "I think that virtual lab is great. I honestly feel that what I was missing from the MSIS program was more hands-on activities. For people that have an MIS background the core courses help reinforcing our current knowledge, but the labs help us know what we need to know in today's market. I have seen my labs overlap my job duties and I am grateful for that. That assures me that what I am learning is very useful."
- "1) Its available when needed even if a class is not in session 2) updated with the latest technology 3) don't really need admin rights to install the software needed for class. "

The virtual lab is also being used in the Database and Decision Support Systems (INSS 650) in spring 2010, where 17 students have access to the multi-users Oracle 10g DBMS. Students are expected to complete four individual SQL assignments and to implement databases for their group semester database projects.

4. Challenges

Creating, configuring and maintaining the virtual machines require a lot of time, financial resource and efforts. It also requires a full support from the university IT leaders and engineers.

Some of the challenges faced by the faculty responsible for the virtual lab are:

- Some students misuse the lab by installing games and software for other courses. Developing a good use policy and enforcing it is crucial.
- A security breach that may originate from the Lab is another concern.
- Some labs require large disk space and create a high demand on the disk space of the host.

Some of the challenges faced by students while using the virtual lab are:

- Students in their journals indicated that sometimes the remote connection is slow. A few examples are: "slow response from Oracle; sometimes it freezes".
- Student's remote desktop connection was timed out while research to complete assignments.

IV. CONCLUSION AND FUTURE WORK

We presented the approach and the technologies used to develop a virtual laboratory (VLAB) that supports information assurance courses mainly delivered in online mode. The VLAB allow students to have different roles such as hackers, security administrator and manager, end-users, and security auditor, and develop IA skills required in the workplace. Students and faculty have access to the lab from anywhere 24/7 using the Internet.

We are working to include reservation system for coordination of accesses to prevent resource conflicts as well as the development of detailed lab support procedures and usage policy. Finally, there is a need to develop a Web-based lab portal that provides a visual depiction of the different components labs.

ACKNOWLEDGMENTS

This work is supported by MHEC grant. We would like to thank Edward Smith, the Network Administrator at BSU, for his technical supports and Dr. Al Valbuena , vice president for IT of BSU for his supports. We would also like to thank the three reviewers for their comments.

V. REFERENCES

[1] S. Patel and J. Stephenson, "BRAC Higher Education Study," Maryland Higher Education Commission, Annapolis, 2008.

[2] Hay and K. L. Nance, "Evolution of the ASSERT Computer Security Lab," Proc. The 10th Colloquium for Information Systems Security Education (CISSE), pp. 150-156, 2006.

[3] T. Zlateva, L. Burstein, A. Temkin, A. MacNeil, and L. Chitkushev, "Virtual Laboratories for Learning Real World Security," Proc. The 12th Colloquium for Information Systems Security Education (CISSE), pp. 150-156, 2008.

[4] VMware, "ESX and vCenter Server Installation Guide," 2009, Accessed on February 10, 2010 from http://www.vmware.com/pdf/vsphere4/r40/vsp_40_esx_vc_installation_guide.pdf.