Global Journal of Enterprise Information System

Incorporating Lab Experience into Computer Security Courses: Three Case Studies

Joon Son[1*], Vijay Bhuse[2], Lotfi Ben Othmane[3] and Leszek Lilien[4]

[1]*Information Decision Science, California State University San Bernardino, USA; json@csusb.edu*
[2]*Department of Computing, East Tennessee State University, USA; bhusev@mail.etsu.edu*
[3]*Center for Advanced Security Research, Darmstadt, Germany*
[4]*Department of Computer Science, Western Michigan University, USA*

Abstract

We describe different approaches taken to teaching security labs at ECPI University (ECPI), University of Maryland University College[28] (UMUC) and Western Michigan University (WMU).These three approaches are then compared in various perspectives such as the type of the educational institution offering them; the lab platform, its accessibility and performance; instructional support and materials; software installation and configuration effort; as well as cost and implementation issues. We believe that an academic institution designing and building a security lab would benefit from reviewing our comparison and examining all three approaches: a pure virtual lab at UMUC, the traditional physical computing lab at WMU, and a hybrid approach at ECPI University. Selecting the appropriate deployment model should then be based on the individual institutional requirements. In addition, we briefly present the challenges we faced and lessons we learned while integrating security labs into the curriculum. Finally, we provide our rationale and conclude that security labs should be an essential part of the curriculum.

Keywords: Computer Security Education, Cyber Security, Hacking, Network Security, Security Challenges, Security Labs, Virtual Cyber Labs

(**Date of Acceptance:** 02-01-2015; **Plagiarism Check Date:** 08-01-2015; **Peer Reviewed by Three editors blindly:** 30-01-2015; **Reviewer's Comment send to author:** 5-02-2015; **Comment Incorporated and Revert by Author:** 5-03-2015; **Send for CRC:** 8-03-2015)

1. Introduction

The frequency and impacts of security attacks are creating an urgent need for training security professionals. ECPI University (ECPI), University of Maryland University College (UMUC), and Western Michigan University (WMU), like many other educational institutions in the United States and abroad, offer courses on computer security[14,27]. Students learn the fundamental security concepts and skills during the courses.Using security labs as a pedagogical tool in the training of students is a common practice[1,9,31]. Our courses also incorporate labs, so students can apply knowledge acquired in the lectures and homework to maximize the learning benefits.

In the computer security labs, the theoretical concepts covered by lectures are followed by hands-on practical activities (or simulations whenever appropriate or necessary). Instructors provide a broader perspective and connections to the learning objectives of the course. Lab activities enable students to contextualize notions in the real-world settings, in a particular domain or a situation, and relate them to their own learning objectives (or at least to the objectives declared by the lab assignments).

Our goal in offering lab experience to students is to assure that they attain at least Level 3 of the Bloom et al.'s taxonomy of the cognitive domain[3], namely Application (based, in turn, upon Knowledge and Comprehension; and underlying, in turn, Analysis, Synthesis and Evaluation). It is a commonly held belief that students learn more efficiently when engaged in a higher order thinking. Hands-on lab exercises provide the means to challenge students with such higher order tasks.

This paper outlines our experience with security labs taught by us: we describe the setup of the labs, the lab assignments, the challenges we faced, and the lessons we learned. We also emphasize the value of security labs in training security professionals, and the need to train well-rounded professionals. This paper extends our earlier paper[19]; it adds the discussion of the security lab experience gained at the University of Maryland University College, and compares teaching approaches at the three universities in terms of the type of the educational institution offering them; the lab platform, its accessibility and performance; instructional support and materials; software installation and configuration effort; as well as cost and implementation issues. It is interesting that the three universities have different delivery

*Author for correspondence

methods for teaching cyber security courses. Western Michigan University offers a traditional face-to-face security course with a physical lab while UMUC provides 100% online security courses to students with a virtual lab using server virtual technology[31,32]. ECPI University uses a hybrid learning method (both physical and virtual lab are available to students and instructors) to teach its information security courses. We believe that the range of delivery methods makes this comparison more insightful for educational organizations building a new security program or improving their existing security courses.

2. Description of the Security Labs

This section describes the lab setups and the projects or assignments for our security courses.

2.1 Security Lab at ECPI University

ECPI University is a private institution established in 1966 and offers in-seat and online AS, BS and MS degrees in Computer Information Sciences. These programs are accredited by the Commission on Colleges of the Southern Association of Colleges and Schools[6]. Students in the bachelor's degree in Computer and Information Science program learn how to manage projects, design and write different computer programs, create web pages, use and maintain databases, and install and secure computer networks. Students also learn to provide customer service when assisting customers and clients with technical issues[7].

2.1.1 The VCASTLE Lab at ECPI

The Virtualization, Cloud, and Storage Technology Learning Environment (VCASTLE) platform at ECPI University[27] offers network security, virtualization, and storage labs to in-seat and online students in Computer and Information Systems (CIS) programs. VCASTLE includes the Network Development Group NETLAB+, VMWare ESXi, Microsoft and Linux Client/Server, Cisco UCS, Routers/Switches, ASA Firewalls, and EMC Storage/Disaster Recovery Systems.

This advanced technology is very effective because it allows to offer to students anywhere (as long as they have an Internet access) diverse lab setups—with various operating systems, routers, switches, firewalls, virtualization, and storage. Remote and anytime access to labs maximizes the university's investment in equipment and software, and gives students full lab scheduling flexibility.

2.1.2 Use of the VCASTLE Lab for Computer Security Courses at ECPI

The VCASTLE system allows an instructor to design and configure multiple computer security lab environments and make them available to students anywhere and anytime. Students log into the lab portal from a web browser, and schedule accesses to their own equipment topologies (Figure 1). Configurations defined by students are saved in a persistent environment.

The VCASTLE-based network security lab comes with a BackTrack[2] Linux machine, which has the latest tools required for penetration testing. BackTrack itself includes information gathering tools, web crawlers, database analysis tools, tools for network mapping and operating system fingerprinting, vulnerability assessment and exploitation tools, as well as password cracking tools. BackTrack comes with Armitage—a front-end for the Metasploit penetration testing software[23].

ECPI University is also a Cisco Networking Academy[15]. As part of Cisco Networking Academy classes we use a simulator named Packet Tracer[20] for simulation, visualization, authoring, assessment, and collaboration (Figure 2). It facilitates teaching of complex networking concepts and networking system design. It also helps with hands-on demonstrations.

2.1.3 Lab Assignments at ECPI

The lab assignments for students use either the actual networking equipment (with Windows or Linuxservers), or a VCASTLE environment to create a network, to experiment with network behavior, and to troubleshoot problems. This learning environment is especially important in demonstrating network security concepts, such as virtual private networks, port security, access control lists, intrusion prevention systems and AAA (authentication, authorization and accounting) servers. The labs help students to develop also general skills such as decision making, creative and critical thinking, and problem solving.

We emphasize hands-on learning and practical aspects of network security especially in teaching undergraduate courses. For example, in one of the network security courses that includes

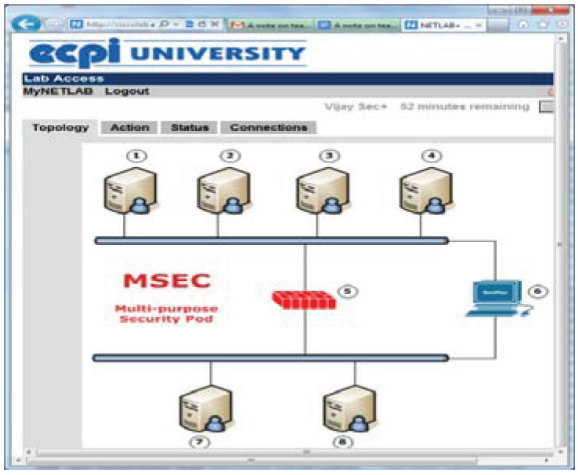

Figure 1. The VCASTLE front end at ECPI.

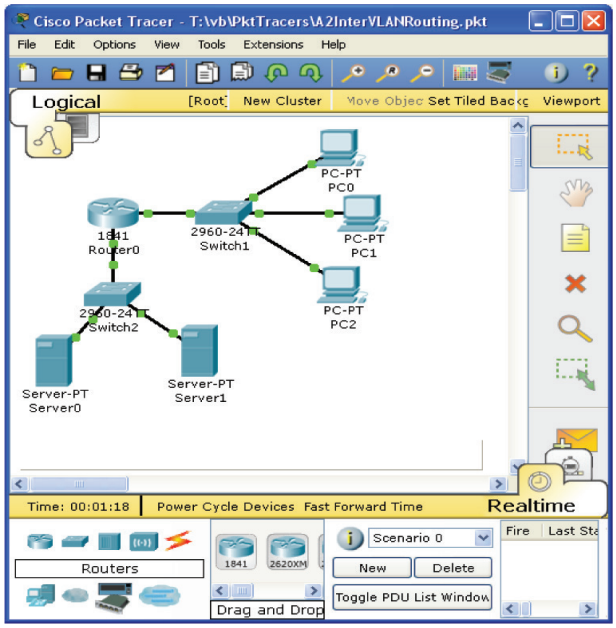

Figure 2. Network simulation with access control using Cisco Packet Tracer.

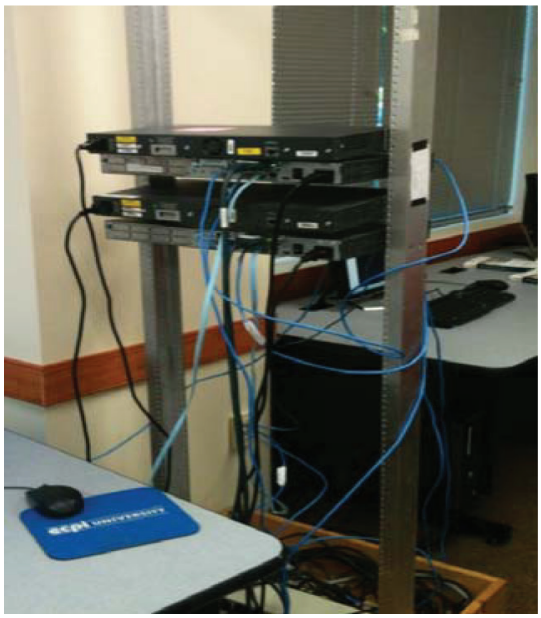

Figure 3. Hands-on learning emphasized with switches and routers.

presenting the concept of an Access Control List (ACL), the students are tasked with constructing an enterprise network consisting of three different domains, and then building a security policy using an ACL to regulate an access between the domains. Figure 3, shows the network devices—switches and routers—used by students to build the network and enforce its security policy.

2.2 Security Lab at UMUC

University of Maryland University College (UMUC), founded in 1947, is a distance learning university, offering a convenient online education from a respected state university. It is the largest public university in the U.S. with over 90,000students enrolled in undergraduate and graduate programs. UMUC has been offering online courses extensively since 1985.

Spurred by the increasing demand for highly skilled cyber security professionals, UMUC began offering its online cyber security Master's degree program in Fall 2010. This required launching a virtual cyber laboratory. UMUC's online cyber security undergraduate program has not yet begun incorporating the virtual lab into its security curricula. Currently, our undergraduate students use an online remote lab where they can access various simulation tools. To use real security tools, they have to install them on their own PCs.

2.2.1 *Virtual Cyber Labs at UMUC*

Knowing the importance of hands-on labs in technology-based courses, UMUC—committed to distance learning—decided to build online hands-on labs (often called virtual labs) to supplement its online cyber security program. Several institutions have implemented virtual labs and each virtual lab platform is specifically tailored to meet their needs[4,8,11,12,22,26,32-34].

UMUC had the following four design goals for the virtual lab:

1. The remote virtual servers must reliably serve a great number of concurrent users with limited dedicated resources. This is a very critical requirement since students from at least 10 to 15 sections must use the virtual lab each week and finish the lab assignment without any significant performance issue. This means the virtual servers should support at least 200~250 concurrent virtual machines. An operating system (e.g., Windows XP, Windows Server 2008, Linux, etc.) is installed and run on each virtual machine.
2. Online lab access must be available around the clock, 365 days a year. This means that students will not have to reserve a time to use virtual resources.
3. The Virtual Machine (VM) must be configured with the appropriate operating system(s) and images including the required security tools to support lab exercises. In order to minimize requirements for students (e.g., configuring or installing software on their own machines), a pool of Virtual Machines (VMs) along with a cloud based network access were deemed necessary.
4. Students must have privileged access rights on the virtual machines to use security or network tools. This implies that students may potentially abuse system resources intentionally or unintentionally. As a result, the virtual lab environment must be monitored to avoid or mitigate adverse consequences.

To satisfy the above requirements, UMUC used an automated virtualization technology called VMware vSphere[30] to build the cyber security lab. One of the major components of vSphere is a hypervisor called ESX or ESXi. This hypervisor, running on an ESX/ESXi host server, is responsible for the creation of virtual machines (VMs) on the host server, as shown in Figure 4.

The VMware vSphere virtualization technology, coupled with cloud-based access, provides the ability for lab applications to be dynamically available to our students. Operating system images, preconfigured for labs and equipped with security tools, can run as VMs. A student can remotely access the virtual lab environment, load one or more preconfigured operating system images, run them as a set of VMs, complete lab assignments, and exit the system.

Since the initial deployment of the virtual cyber security lab, a number of performance improvements have been made to support up to 300 concurrent virtual machines. vCloud Director[30], a virtual management service, allows for several features including the creation of separate networks (called virtual networks) within the virtual lab. The virtual networks provide a separate workspace for each student as shown in Figure 4.

When a student logs on and begins a lab exercise, virtual machine templates (with pre-configured software and tools) are automatically generated. The virtual network and virtual machines are accessible via the student's account and are made available through vCloud Director's web interface.

In a typical semester, approximately 1,000 graduate students are required to participate in at least two online virtual labs for each of their five technical courses. Although some attempts have been made to avoid having overlapping labs, this is not always feasible because of the nature of the 12-week long graduate term. For example, during some weeks there may be two or more different courses, each consisting of 10 to 20 sections, accessing the virtual labs.

Figure 5 displays the number of VMs running and used by students in the week of September 17 to 23, 2012.It shows that the UMUC virtual cyber lab environment is capable of providing a reliable 24/7 access, and supporting over 200 concurrent VMs (e.g., about 220-230 VMs were running concurrently at 6:30 p.m. on September 23, 2012).

To maximize students' learning experience, one professor and one lab assistant are assigned to each section. The primary job of a lab assistant is to help students with any issues they may encounter while doing lab activities. The typical issues are VPN connection problems, web browser compatibility/configuration issues, students' confusion or misunderstandings of the lab manuals, etc.

Virtual labs are used for online security courses, as illustrated here with two security lab examples.

2.2.2 *Lab Assignments at UMUC*

We illustrate lab assignments at UMUC with the following examples.

Example 1 – Lab assignment experimenting with Snort and Wireshark for Intrusion Detection.

This lab assignment is intended to provide experience with the Snort and Wireshark programs. Just like the vulnerability scanning lab assignment, students make a VPN connection to the virtual cyber lab and import a VM. The VM is already preconfigured with Snort, Wireshark and a sample packet trace file. First, students should look through the packet trace file using Wireshark, and create 6-8 snort rules that will uniquely identify the 6-8 different packet signatures. To complete the LA, students must run Snort with a set of appropriate flags and the snort rules

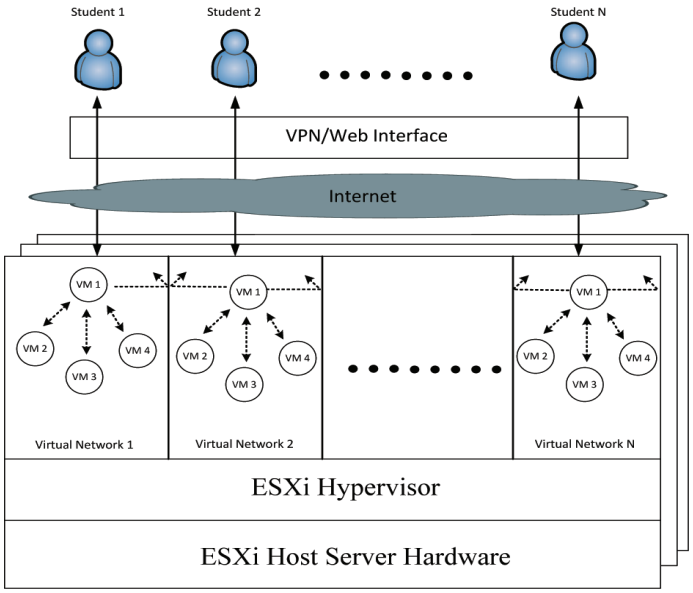

Figure 4. Virtual Lab with a set of virtual networks at UMUC.

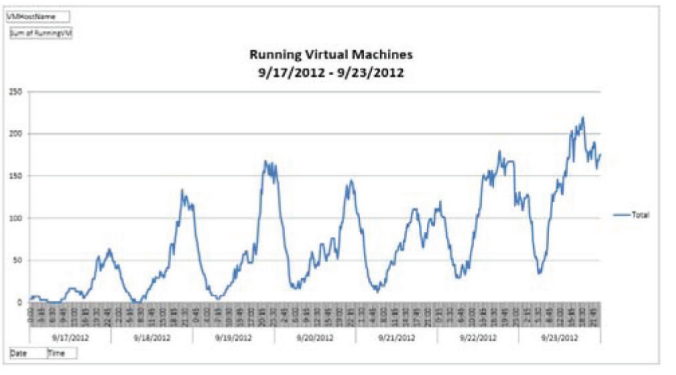

Figure 5. The number of virtual machines running during the week of September 17 to 23, 2013.

GJEIS | Print ISSN: 0975-153X | Online ISSN: 0975-1432

they created. A complete video tutorial as well as lab manual are available for students.

Example 2 – Vulnerability scanning lab assignment

A vulnerability scanning LA is shown here as an example of how the current UMUC virtual lab is used by students. In this lab assignment, students first make a VPN connection to the UMUC virtual lab environment. Through the vCloud Director's web interface, each student imports four OSs and runs the OSs as VMs in her/his own workspace (virtual network).

The example in Figure 6 shows the menu panel with three console icons visible: for VM1, VM2, and VM3; in addition, VM4 is hidden under the right-arrow to the right of the icon for VM3. VM1 with Window XP is used as a client machine to scan the remaining three VMs. VM 2 is a Window 2008 server providing services such as FTP, Telnet, HTTP, HTTPS, MySQL. VM 3 and VM 4 are Linux servers running services such as FTP, HTTP, SSL, HTTP, MySQL, and DNS.

The primary goal of the lab assignmentis to provide students with an opportunity to experiment with Nmap and Nessus[16,18,23] in order to identify network vulnerabilities in VM2, VM3, and VM4. To successfully complete the LA and answer its exercise questions, students must experiment with many features of Nmap and Nessus. Figure 7 shows one of Nmap features used by students to answer questions for an LA.

Since each student effectively has own virtual network that is isolated from every other student's network (Figure 4), any malicious activities or non-intended network traffic will be contained and restricted to that user's workspace and virtual network. This is one of the major benefits using virtual networks (through vCloud Director).

2.3 Computer Security Lab at WMU

Western Michigan University (WMU), founded in 1903, with nearly 25,000 undergraduate and graduate students is one of the top-100 public universities in the United States, and among the nation's top "research universities" as classified by the Carnegie Foundation for the Advancement of Teaching[25].

The Department of in Computer Science offers in-seat programs only[5]. Students in the B.S. program in Computer Science, accredited by the Computing Accreditation Commission of ABET, are provided with a solid foundation preparing them for analysis and design of software, hardware, and systems. The M.S. in Computer Science program emphasizes computer software development and theoretical foundations of computer science.

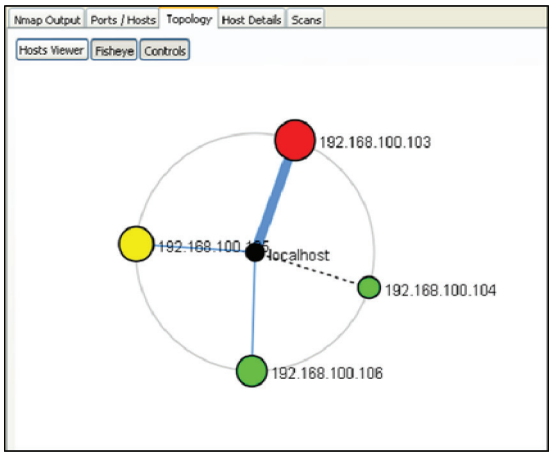

Figure 7. The Nmap security scanner showing the topology diagram of the virtual network assigned to a student.

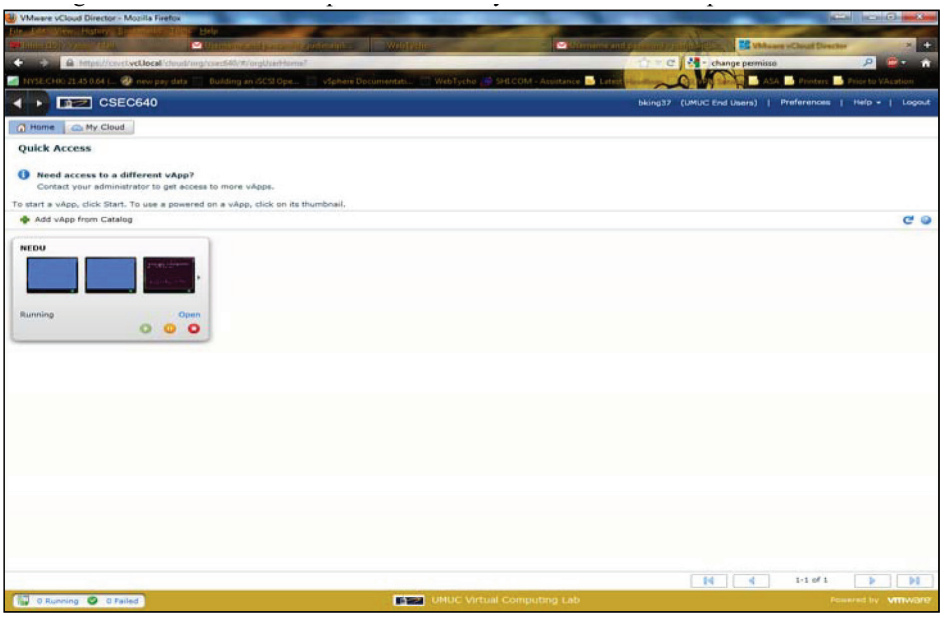

Figure 6. Loading a set of VMs via the web interface of the vCloud Director.

Graduates of this program, in addition to receiving a strong theoretical background, should also become competent programmers and system designers. The plan of study for the Ph.D. degree allows for considerable variety of focus; students can take advantage of the strengths of the department in matching their interests (Department, 2013).

2.3.1 The Computer Security Lab at WMU

The lab is composed of 15 desktops; one desktop is used as a server and the remaining 14 are used by students as clients. Each desktop runs up to three virtual machines (VMs) managed by Microsoft Virtual PC[29], as illustrated in Figure 8. Till Fall 2013, each VM used the following operating systems (OSs): Windows X Pro, Ubuntu 6, and Windows 2008[a]. Each VM has a unique network configuration and can communicate with the other VMs, including the VMs of the servers. The server runs a Postfix email server[21], an FTP server (included with MS Windows), and has a shared folder for the tools that students need in their labs.

To avoid contamination of the Internet by run-away malware that could be experimented with in the lab, the lab network is fully independent, with its own DNS server, etc. To allow for a controlled, secure access to the Internet, it is permitted via a single designated port.

2.3.2 Use of Computer Security Lab for Computer Security Courses at WMU

The Computer Security Lab at WMU[13] is used in the advanced in-seat undergraduate course: Computer Security and Information Assurance, which is optional in the B.S., M.S. and Ph.D. programs in Computer Science. The lab can also be used in the in-seat graduate course Advanced Computer and Information Security, as well as various independent-study courses.

2.3.3 Lab assignments at WMU

The lab assignments help students to develop and test not only computer networking and security skills, but also much broader skills, such as creative and critical thinking, problem analysis and solving, accuracy and being attentive to details.

The lab assignments[13] are based on security experiments described by Nestler et al. in their Computer Security Lab Manual[17]. In the four preliminary assignments, the students experiment with a set of commands and tools to gain knowledge on and skills for OS and network protocols used in the lab. For instance, they install and configure Windows XP Pro, Ubuntu, and Windows 2000; use network tools to observe TCP handshaking; use command-line interface to send messages using the SMTP protocol; and use network commands, such as netstat.

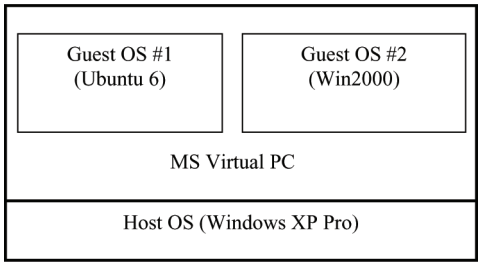

Figure 8. The VMs structure in the Computer Security Lab at WMU.

In the remaining, security-related assignments the students: (i) experiment with tools for IP scanning and Windows vulnerability scanning, such as Nmap[23] (ii) practice resisting malware attacks, including denial of service (DoS) attacks (e.g., SYN flood attacks); (iii) perform attacks that exploit vulnerabilities in Windows 2000 (e.g., using a well-crafted URLs that exploit Internet Information Service vulnerabilities), then install patches that harden this OS; (iv) run malware software and investigate its behavior (our lab is completely separated from the Internet to prevent adverse effects of this experiment on the outside world, as explained above); and (v) experiment with Snort, an intrusion detection tool[23].

3. Comparison of Three Security Lab Approaches

In this section, we summarize and compare three different approaches to computer security labs to identify their characteristics based upon the following attributes:

1. Type of educational Institution: it depends on the type of the programs the institution offers, including academic degrees granted (e.g., B.S./M.S.), educational delivery methods (e.g., distance learning, a traditional in-seat program, or a hybrid program).
2. Lab platform, its accessibility and performance: this answers the questions like "Does a student use a virtual lab or a traditional physical lab?" or "Is there any interaction latency a student experiences?".
3. Instructional support and materials: this refers to issues an instructor faces when creating teaching material and learning environments.
4. Software installation and configuration effort: this discusses a level of effort to configure or maintain a security lab environment, including any issues related to software licenses and resolving license conflicts.

[a]Currently, we use Windows 8 and Windows Server 2008.

Table 1. Comparison of three computer security lab approaches. LA = Lab Assignment

Type of Educational Institution	Lab Platform, Its Accessibility and Performance	Instructional Support &Materials	Software Installation and Configuration Effort	Cost& Implementation Issues
Western Michigan University (WMU)				
* Traditional university (with a relatively few distance learning programs). * BS, MS and PhD degrees in Computer Science(no online degree programs in Computer Science).	* Traditional physical computing lab (PLAB) environment. * Access to the lab during the operating hours. Either an instructor or lab assistant must be present during the lab hours. This is one the major disadvantages of PLAB. * Performance depends on PCs available in the lab. However, students do not experience network delays.	* Available quick feedback from a lab attendant (help with hardware or network issues). * Set of detailed lab scenarios based on a published lab manual[17] * A prepared demo can be shown (on request) so students feel less pressure in acquiring information from an instructor.	* First LA teaches the student how to install network & security tools. * Since a few lab PCs have a different hardware configurations, a small number of students face some issues in tool installation. * Using the client VM technology to overcome the different configuration and installation issues. A virtual image prebuiltby instructors is already installed in each lab PC. * The prebuilt image cannot be freely distributed to students because of distribution agreements for commercial software tools & OS. This means students can use the commercial tools only in the lab.	* The Department of Computer Science has a lab facility and lab administrator. *The cost of building a lab depends on many factors, including space availability, a number of PCs, servers, and network devices (such as routers, switches, and firewalls, etc.).
University of Maryland University College (UMUC)				
* Non-traditional online program. * BS andMS degrees in Cyber Security. * High enrollment (UMUC cyber security undergraduate and graduate programs enrolled over 4,200 students in Fall 2012 (UMUC at a Glance, n.d.), and more than 400 students earned their MS degree in 2013[10].	* Virtual computing lab (VLAB) environment. *Access the lab anytime anywhere. *Students geographically located in all 50 states and 20 countries. * Supports over 20concurrent virtual machines (VMs). However, as the number of deployed VMs reaches a threshold point (i.e., more than 200 VMs), response delays occur.	* Immediate help not possible. However, each section (about 20 students) has a dedicated lab assistant. Typically, the dedicated lab assistant responds to any lab-related issue within 24 hours. This significantly eases the burden on the instructors. * A detailed and step-by-step lab instruction provided for each lab. Many multi-media lab instructions are also available. * Instructors spend a lot of time preparing lab manuals to help students who have no immediate help for their LAs. *An instructor can monitor and help students' lab activities as a root user. * Instructors and course designers work with a lab specialist whose sole responsibility is to monitor the virtual lab performance and to educate the lab assistants.	* For each LA, a set of VM images, prebuilt withcommercial or open tools, is automatically loaded. * Easy to identify and manage the scope of software licenses and payment of fees— since UMUC takes care of it. UMUC contacts the software vendors to resolve any legal issues if their product is used in its VM environment.	* The total cost of supporting at least 250~300 concurrent VMs without significant performance degradation is very high. * The total cost of a virtual lab increases exponentially as the performance requirements (the number of concurrent VMs) increase.[b] *It is often a challenge to provide a user-friendly and secure web interface to the virtual lab. The reason is that the web interface does not support every available browser, and students keep updating browsers to their new editions.

(Continue)

ECPI University				
* Traditional and Online University. * BS and MS degrees in Network Security.	* Hybrid lab environment: PLAB and VLAB. * Instructors have an option to choose either PLAN or VLAN, depending on their needs. * No requirement that a significant number of concurrent users must be served (since a typical IT course includes both PLAB and VLAB). Performance limitation (e.g., a number of concurrent virtual machines) of the VLAB not tested yet.	* Typically instructors use VLAB in class to help students with configuration or installation issues. * Students access VLAB when the PLAB is closed in order to do LAs or practice what they learned in class. * Since most of IT courses are in-seat, students can easily get an immediate assistance from their instructors. However, no immediate help is available when students access VLAB and face problems outside of the classroom.	* If a lab requiresusing commercial security tools, an academic bundle license is purchased and the tools are installed on the VM. Students are advised to use VLAB to use the commercial tools for carrying out their experiments when they cannot come to the PLAB during lab hours. * Easy to manage the scope of distribution agreements for commercial software if VLAB is used. * Simple lab assignments, requiring limited configuration and installation effort, can be performed in PLAB.	* The cost of building a VLAB is a lot less than UMUC' VLAB since no significant performance requirement regarding a number of concurrent users or VMs.

[b]For example, constructing a virtual lab able to reliably support 300 concurrent VMs will easily cost one million dollars. The major component of the total cost is a SAN (Storage Area Network) array

5. Cost and implementation issues: considers cost or implementation issue associated with building and maintaining a security lab.

4. Challenges and Lessons Learned

The following are the main challenges we encountered in our security labs, and the lessons we learned addressing them.

4.1 Lab Isolation

The main issue in designing security labs is isolating the lab hosts from the university network (and other external networks) while using some of the same network infrastructure. This assures that no accidental damage is done (e.g., malware does not infect the university or another external network) even if, for example, the lab connects to the Internet and Domain Name Service (DNS) servers.

If malware lab experiments are done inside VMs, there is a very small probability that any malware used in the experiments "escapes" from the lab, spreads through the university network or the Internet at large, and infects hosts outside the security lab. But there exist malware that affects host machine even if it is installed only in a VM. So, while performing experiments with malware it is very important to take extra precautions that it will not spread beyond the lab setup.

At ECPI, the security lab's network is physically separated from the university network, and the machines in the lab are not directly connected to the Internet (instead, they are connected only to the internal network and internal DNS servers).

At UMUC, once a student user logs into the virtual cyber lab, the student is automatically assigned a virtual network through the virtual management service (vCloud Director). Effectively, each student has an own (virtual) network that is isolated from every other student's network. Any malicious activities or unwanted traffic originating from a user will be restricted to that user's workspace and virtual network.

At WMU, the network is fully independent, with its own DNS server, etc. However, the hosts can connect to the Internet through a single designated port.

In our experience, all these approaches work well in practice.

4.2 Design of Lab Assignments

Designing attack scenarios for experimentation in a security lab requires a deep knowledge about operating systems, network protocols, etc. In turn, performing attacks requires time to carefully execute the attack steps.

After several attempts of executing lab assignments, we learned: (i) to use virtual technologies and preconfigured images of hosts—so students spendless time when installing and configuring operating systems on their hosts; (ii) to teach students the requisite background knowledge and theory—so they understand the attack steps, the tools, and the outcome of each step; and (iii) to carefully select the lab exercises—so students get the maximum benefit during the time they can allocate to each lab assignment.

4.3 Unexpected Exercise Results and Student Support When They Occur

A major sources of unexpected exercise results are non-uniform execution environments used by students. This includes non-uniform hardware (e.g., some PCs used network cards that replaced the nonfunctional original ones) or non-uniform software environments.

We believe that we have eliminated the latter source of unexpected exercise results, namely having diverse software execution environments. We have done so with the support of virtualization technologies and downloading uniform images into students' execution environments. Since virtualization technologies allow students to use an image prebuilt with the same set of security tools, a number of unexpected exercise results can be significantly reduced.

Two most popular virtualization technologies to support cyber security labs are: (i) server-side virtualization for running the virtual machines on a remote server; and (ii) desktop virtualization (a.k.a. client virtualization) for running virtual machines on user's own personal computer.

A cyber lab with server-side virtualization facilitates selection and importing of preconfigured images designed specifically for each lab assignment. However, the major disadvantages of server-side virtualization are cost and performance. An initial cost to build an online cyber security lab could be substantial due to the need for an extra hardware (e.g., high-performance remote servers, Storage Area Network (SAN) arrays, SAN switches, other routers/switches, etc.) as well as extra software. In addition, if a lab needs to support a large number of concurrent users or a significant number of concurrently running virtual machines, constant monitoring of remote virtual servers and performance tuning are essential.

The server-side virtualization is used in the security/network labs at ECPI and UMUC. The preconfigured images provided to all students for a given lab assignment include the same set of security and network tools and test files. This assures that students seldom encounter any unexpected results—if only they faithfully follow lab manuals. In addition, the instructors or lab assistants are given an administrator privilege and can access and view the VMs used by the students in class. This allows the instructors and lab assistants to monitor students' lab activities whenever they wish to do so.

In contrast, at WMU, the desktop virtualization is used. This is less expensive and eliminates the need for constant performance monitoring and tuning. This would create problems if students wanted to run lab exercises outside of the security lab room.[c]

Another major source of unexpected exercise results, which cannot be prevented with virtualization, are system changes resulting from performing experiments. Maybe the most frequent cases are a result of students deviating from exercise specifications provided by the lab manuals (which mentioned above). This is a human factor impossible to fully control in a way other than penalizing such deviations with a lower grade.

Other cases of producing unexpected exercise results due to system changes resulting from performing experiments come from the fact that the execution of attack steps changes the state of the attacked host. For example, a student who hardens a VM and installs the SP2 patch for Windows XP cannot use the tool to perform a DoS attack on the hardened machine, since SP2 prevents such an attack. This shows that a small change in instructions for a lab assignment may results in an outcome completely different than the expected one.

Moreover, even though all hosts in the lab have identical or very similar hardware and software, we are faced with situations when exercises on some hosts produce results different than on others. The instructors or the teaching assistants for the lab have to spend time to investigate the causes and find solutions. Since the problems can reoccur, we maintain a knowledge base of these problems and their solutions; it was in the form a web page available to the students.

We need to remember to warn students about the above issues and nuances that can lead to unexpected results.

4.4 Grading Unexpected Results

In some cases students reported unexpected outcomes of their lab assignments, which made it more difficult to fairly judge their work (esp. in the view of the preceding challenge/lesson learned).

In such cases, we learned to ask the affected students for lab assignment demonstrations, so they could show how they performed the exercises. The demonstrations allowed us to assign a fair grade—after understanding the causes of the unexpected results (or, at least, after eliminating the possibility that the cause is due to a student's mistake).

[c]First, the students may have a problem installing desktop virtualization software or running VMs on their PCs. Second, the desktop virtualization approach may not scale well for labs requiring multiple VMs. For example, the vulnerability scanning lab (shown in Example 2 above) requires at least 3 to 4 GB RAM (8GB of RAM is recommended). Not all students' personal computers were powerful enough at that time to execute 4 to 5 VMs. Third, it is not easy to identify and manage license issues. There could be many such issues if commercial OS images and tools were distributed to students. To avoid worrying about licensing, a Linux image including non-commercial tools may be provided to students.

4.5 Impact of New Software Versions

Lab assignments involving hacking rely on exploiting vulnerabilities of specific versions of specific software, such as MS Windows 7, Adobe Acrobat Reader, or the BackTrack application. In this context, new versions of software can produce unexpected results, even derail some of the lab experiments, which were earlier performed successfully.

In some cases, the new version of software fixes vulnerabilities exploited by known attacks. We use these cases to experimentally demonstrate to students how software updates can improve computer system security.

5. Discussion and Conclusions

5.1 Hacking and Deep Understanding of Computer Security

There is a danger that network security education considers security as a cat-and-mouse game, and focuses solely on teaching specific "hacking" tools and skills to detect and protect from only a narrow set of known attack categories. Hackers trained in this way are able to identify system and software vulnerabilities. However, too often their knowledge is limited to the threats they know. In particular, they do not have enough expertise to build more secure systems[24]. To avoid this trap, we train our students not just in "security hacking" but also in a broad range of fundamental security concepts, challenges, and skills.

However, we agree that "just hacking" can be used to create excitement in existing security labs and to attract students to study computer security in depth. Therefore, some "hacking" is included in our lab assignments, For example, we hope to resume offering applied system security and applied network security courses for undergraduates at WMU—both with significant "hacking" contents.

Hacking security labs help students to understand the complex security concepts more deeply via the hands-on practice with the attack and defense techniques under the condition that the emphasis is on the concepts and not the exercises themselves. This facilitates connecting the theoretical concepts that students learn from the computer security lecture as well as other lectures on information systems (e.g., on computer networking).

Incorporating hacking-based lab assignments is a challenge for instructors especially if they use specific versions of an application software or an operating system. The instructor must update labs periodically to keep up with the application and operating system updates and releases of patches and service packs.

5.2 Lab as a Motivator and Lab Expenses

Having security labs (even without a visible hacking experience) motivates students to take security courses that contain them. At UMUC, it is commonly observed that a well prepared lab attracts more positive feedback from students on course evaluation. At WMU we found it the hard way: the number of students who registered for our security course was reduced considerably when (due to lab rebuilding problems) we had to offer the course with a very limited security lab component.

Providing this motivation requires a significant investment for an academic institution. A lab for in-seat or online students requires a considerable amount of hardware, software, network bandwidth, physical space, as well as installation and management and efforts. There is not only an initial cost to set up the lab but also an ongoing expense due to maintenance and keeping the lab up to date. Therefore it is important to have a proper strategy and long-term plan.

5.3 Summary and Conclusions

We summarized and compared via various perspectives different approaches taken by ECPI, UMUC and WMU to teaching security labs. We presented the challenges we faced and lessons we learned while teaching security labs.

We believe that an academic institution designing and building a lab would benefit from reviewing our comparison table (Table 1), and examining all three approaches: a pure virtual lab at UMUC, the traditional physical computing lab at WMU, and the hybrid approach at ECPI. Selecting the appropriate deployment model should then be based on the individual institutional requirements.

We can also conclude that although creating and maintaining a security lab requires a long-term plan and a significant cost, it should be an essential part of the computer science or information technology curriculum since security labs: (i) motivate students and improve retention; (ii) reinforce broad understanding of security concepts and challenges; and (iii) increase enrollment in security courses.

5.4 Disclaimer

All the views and opinions in the paper are based on Author's perceptions and they do not represent an official position of the affiliated institutions.

This work was supported, in part, by the Hessian LOEWE excellence initiative within CASED, and a Fraunhofer Attract grant.

6. References

1. Abler R, Contis D, Grizzard J, Owen H. Georgia Tech information security center hands-on network security laboratory. IEEE Trans on Education. 2006 Feb; 49(1):82–7.
2. Backtrack. BackTrack: penetration testing and security auditing linux distribution. 2013. Available from www.backtrack-linux.org/, accessed in April 2013.
3. Bloom BS. Taxonomy of educational objectives - Handbook 1 The Classification of Educational Goals. 2nd ed. Addison Wesley Publishing Company; Longman, NY: 1984.
4. Burd SD, Seazzu AF, Conway C. Virtual computing laboratories: A case study with comparisons to physical computing laboratories. Journal of Information Technology Education: Innovations in Practice. 2009; 8:55–78.
5. Department of Computer Science. Western Michigan University, Kalamazoo, MI. 2013. Available from https://www.cs.wmich.edu/. Accessed in June 2014.
6. eConnect. About eConnect. 2014.Available at http://www.ecpi.edu/econnect/about-econnect/ Accessed in May 2014.
7. ECPIU. ECPI University - Computer and Information Science, Bachelor of Science. 2014. Available from http://ecpi.smartcatalogiq.com/en/2014/Catalog/Program-Information/School-of-Technology/Computer-and-Information-Science/Computer-and-Information-Science-Bachelor-of-Science. Accessed in May 2014.
8. Fuertes W, Lopez de Vergara JE, Meneses F. Educational platform using virtualization technologies: Teaching-learning applications and research uses cases. Proc. II ACE Seminar: Knowledge Construction in Online Collaborative Communities; 2009 Oct; Albuquerque, NM.
9. Ho JW, Mallesh N, Wright M. The design and lessons of the ASCENT security teaching lab. Proc. 1[3th] Colloquium for Information Systems Security Education (CISSE '09); 2009 Jun; Seattle, WA. p.124–32.
10. IES, Institute of Education Sciences, National Center for Education Statistics. 2012. Available from http://nces.ed.gov/collegenavigator/?q=UMUC&s=all&id=163204#programs. Accessed in February 2015.
11. Li P, Jones JM, Augustus KK. Incorporating virtual lab automation systems in IT education. Proc. American Society for Engineering Education Annual Conf. and Exposition 2011; 2011 Jun; Vancouver, BC, Canada.
12. Li P, Toderick LW, Lunsford PJ. Experiencing virtual computing lab in information technology education. Proc. 10th ACM Conference on SIG-Information Technology Education; 2009 Oct; Fairfax, VA. p.55–9. doi: 10.1145/1631728.1631747.
13. Lilien L. CS 5700 - Computer Security and Information Assurance (CSIA), Spring 2012. Department of Computer Science, Westerrn Michigan University. 2013. Available from http://www.cs.wmich.edu/~llilien/teaching/2012_spr/cs5700/index.htm, accessed in April 2013.
14. Lilien L, Othmane BL. CS Lab 5950: Computer Security and Information Assurance (CSIA), Fall, 2008. Department of Computer Science, Westerrn Michigan University. 2013. Available from http://cs.wmich.edu/~lbenothm/Teaching/Fall2008/CS5950/CSLab5950index.htm, accessed in April 2013.
15. NetAcad. Cisco networking academy. 2013. Available from http://www.cisco.com/web/learning/netacad/index.html, accessed in May 2013.
16. Nmap. Nmap free security scanner. 2013. Available from http://nmap.org, accessed in May 2013.
17. Nestler V, Conklin W, White G, Hirsch M. Computer security lab manual. McGraw-Hill/Irwin; 2005.
18. Nessus. Tenable Network Security, Nessus vulnerability scanner. 2013. Available from http://www.tenable.com/products/nessus/. Accessed in May 2013.
19. Ben Othmane L, Bhuse V, Lilien L. Incorporating lab experience into computer security courses.Proc. Intl. Conf. on Education & E-Learning Innovations (ICEELI 2013). 2013 World Congress on Computer and Information Technology (WCCIT); 2013 Jun; Sousse, Tunisia. p. 1–4. Available from http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?reload=true&arnumber=6618731. Accessed in February 2015.
20. Packet Tracer. Cisco Packet Tracer. 2013. Available from http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html, accessed in May 2013.
21. Postfix. The Postfix Home Page. 2013. Available from http://www.postfix.org/, accessed in April 2013.
22. Rajendran L, Veilumuthu R, Divya J. A study on the effectiveness of virtual lab in E-learning. Intl J. on Computer Science and Engineering. 2010; 2:2173–5. Available from http://www.enggjournals.com/ijcse/doc/IJCSE10-02-06-91.pdf. Accessed in February 2015.
23. SecTools. SecTools.Org: Top 125 Network Security Tools. 2013. Available from http://sectools.org/. Accessed in April 2013.
24. Spafford E. Some thoughts on 'cybersecurity' professionalization and education. 2013. Available from http://www.cerias.purdue.edu/site/blog/post/some_thoughts_on_cybersecurity_professionalization_and_education/. Accessed in April 2013.
25. Standard Listings. Carnegie Foundation for the Advancement of Teaching. 2014. Retrieved from: http://classifications.carnegiefoundation.org/lookup_listings/standard.php. Accessed in March 2014.
26. Tao L, Chen L–C, Lin C. Virtual open-source labs for web security education. Proc. World Congress on Engineering and Computer Science 2010 (WCECS); 2010 Oct; San Francisco, CA. p.280–5. Available from http://www.iaeng.org/publication/WCECS2010/WCECS2010_pp280-285.pdf, accessed in February 2015.
27. Trevethan T. How ECPI university is accelerating educational access, eCONNECT. 2013. Available from http://www.ecpi.edu/flipbook/newsletter/winter-2013/files/assets/downloads/publication.pdf. Accessed in April 2013.
28. UMUC at a Glance (n.d.). Available from http://www.umuc.edu/visitors/about/ipra/glance.cfm. Accessed in February 2015.

29. Virtual PC. Windows Virtual PC. 2013. Available from http://www.microsoft.com/en-us/download/details.aspx?id=3702. Accessed in April 2013.
30. VMware. VMware vCloud Director installation and upgrade guide. 2010. Available from http://pubs.vmware.com/vcd-51/index.jsp?topic=%2Fcom.vmware.vcloud.install.doc_51%2FGUID-F14315CC-B373-4A21-A3D9-270FFCF0A417.html, 2010. Accessed in February 2015.
31. Willems C, Meinel C. Practical network security teaching in an online virtual laboratory. Proc. 2011 Intl. Conference on Security & Management (SAM 2011); 2011 Jul; Las Vegas, NV. p.65–71.
32. Willems C, Meinel C. Online assessment for hands-on cyber security training in a virtual lab. Proc. 3rd IEEE Global Engineering Education Conference (EDUCON); 2012 Apr; Marrakesh, Morocco.
33. Yen T-C. The management of Linux virtual lab by dual load-balancing. Proc. 40th Intl. Conf. on Computers and Industrial Engineering; 2010 Jul. p.1–5.
34. Zenebe A, Anyiwo D. Virtual lab for information assurance education. Proc. 14th Colloquium for Information Systems Security Education; 2010 Jun; Baltimore, MD.

Citation:

Joon Son,Vijay Bhuse, Lotfi ben Othmane, and Leszek Liliend
"Incorporating Lab Experience into Computer Security Courses: Three Case Studies",
Global Journal of Enterprise Information System. Volume-7, Issue-2, April-June, 2015. (www.gjeis.org)

Conflict of Interest:

Author of a Paper had no conflict neither financially nor academically.
In-fact the Authors are highly indebted and acknowledge to the Hessian LOEWE excellence initiative within CASED, and a Fraunhofer Attract grant.