A Concept Focused Security Lab Environment

Steven Fulton and Dino Schweitzer, *United States Air Force Academy*

Abstract – Several educators have noted the benefits of providing students a hands-on experience in security education. Different approaches, such as traditional labs, competitions, virtual labs, and simulated web labs have been proposed. At our institution, we have used a variety of different approaches over the years and have concluded that the best approach depends on the complexity of the concepts being taught and the student background in the area. As a result, we now use a combination of lab approaches based on the subject. This paper will describe the different ways of providing hands-on labs, our decision process for the appropriate format, and our experiences with using this approach.

Index terms – Security education, hands-on security labs

I. Introduction

Information security is a critical area for computing professionals to understand. In recent years, with the increasing cyber threat and prominence of security attacks and vulnerabilities in the media, there has been a marked increase in the emphasis placed on security education. The most recent ACM recommended Computer Science curriculum now includes information security as a core topic in 3 out of 14 fundamental knowledge areas for the discipline [1]. The US government acknowledges the need for increased education as a key component of protecting our national cyber assets [2, 3]. Numerous textbooks, curricula, and educational material have been developed and presented in the literature to support this demand.

Different approaches to teaching security have been presented in the literature. One approach is to integrate topics across the curriculum by adding lessons on security concepts in existing courses at the appropriate place. A different approach is to create separate security courses and/or set up complete programs and concentrations in security. Many educators have identified a laboratory component as an important element of security education, along with the associated logistical and ethical challenges of teaching "hacking" tools [4-8]. The ability for students to get hands-on experience with current tools and techniques is motivational to students and creates an active learning approach to the subject [9]. Some of the challenges associated with creating labs for the security course are the mechanics and cost of creating complex configurations, the headaches of system administration, the need for network isolation, and the inherent risk of providing students with escalated privileges to accomplish necessary system administrative tasks. Security educators continue to grapple with ways to reduce these burdens while continuing to provide hands-on security labs which support their learning efforts. This paper summarizes some of the common lab approaches and describes our method.

II. Background

A. Use of Traditional Labs in Security Education

As previously noted, lecture-based security education courses are often coupled with hands-on labs in an attempt to create an ideal environment in which exercises support in-class lectures. Traditionally, these hands-on labs have been taught in an isolated lab environment which permits the ability to attack and defend systems or demonstrate security related skills without fear of exploitation of on-line systems [10-13]. Several key attributes have been identified as necessary for a well-designed security lab:

- reconfigurable
- heterogeneous
- scalable
- cost effective
- maintainable
- realistic
- insulated

In our experience, a traditional laboratory lab in computer security requires multiple physical systems each with dedicated roles. For example, a security networking environment may include a dedicated root level DNS server, mail servers, web servers, SQL servers, domain controllers and other machines to simulate real world environments. Such a complex laboratory environment requires either a dedicated lab manager to run the lab or substantial amounts of time from course instructors to manage and maintain the lab. Additionally, we have found that as labs become more complex, the hardware and software costs to maintain and upgrade the environment to permit more sophisticated areas of study requires additional funding.

ISBN 1-933510-96-X/$15.00

B. Virtual Machines in Security Education

The concept of virtual machines (VM) has been around since the early days of IBM. Different architectures and operating systems could be emulated through VM software that made the system appear to be a different machine than what it was. Some of the early advantages noted for using VM were that one could execute different operating systems and instruction sets on the same machine; it allowed for the development of software for one machine on a different one; and it provided for insulation of one software environment from another [14].

The use of VM's in education has increased in popularity in recent years due to improved processing power and memory capacities of modern computers; the availability of inexpensive or free VM software; enhanced network bandwidth allowing remote access; and a recognition of the advantages VM solutions offer to systems-level experimentation by students. Some of the key advantages of VM solutions are [15, 16]:

- Cost effectiveness of emulating hardware devices and systems in software versus owning and maintaining large hardware inventories.
- Rapid reconfiguration of networks and systems to create the appropriate architecture for studying the desired tools and concepts. This supports both running different labs in the same course as well as reconfiguring for different courses sharing the same equipment. This not only saves time in administering systems, but allows for repeatability in cases where students need to recover from serious mistakes in their experimentation.
- Isolation from other students and the network population at large. One student's mistakes do not affect the lab experience of other students. "Sandboxing" applications and systems from the general network is critical when experimenting with potentially harmful malware or tools.

Several educators have presented different solutions for how to configure and implement virtual labs to support security education [17-23].

C. The use of Web Labs

In the past several years, we have started the development and use of self-contained Web Labs. Web Labs are usually java-based programs which are typically delivered to students in a web browser. These labs have been developed with the goal of bringing highly complex security topics in an easily accessible way while requiring minimal faculty preparation, lab support, or student background knowledge [24]. Web labs allow complex topics to be presented to students without having to worry about multiple computers or complex computer hardware and software environmental configurations; they simulate experiences instead of demonstrating real life situations on actual hardware and software.

The web labs are designed to be completed within a single class period (typically an hour) and provide a written narrative to walk the student through the given scenario. For example, the Buffer Overflow Web Lab (Figure 1) outlines a simple introduction which sets up the scenario prior to walking the student through the steps which modify memory. Not only is the simulated program shown in C (note the code on the left of Figure 1), the step button allows the student to step through the program code and a portion of memory which hold the associated code is also visible. As changes are made by stepping through the program, the associated changes are made in the memory section as well. Input to the program is provided in the screen area directly below the step buttons. In a traditional lab environment, the execution of the C program would have to be done in one window while a second window would be required to follow changes to memory. This simplified simulated approach makes the concepts associated with buffer overflow much easier for the novice student to follow.

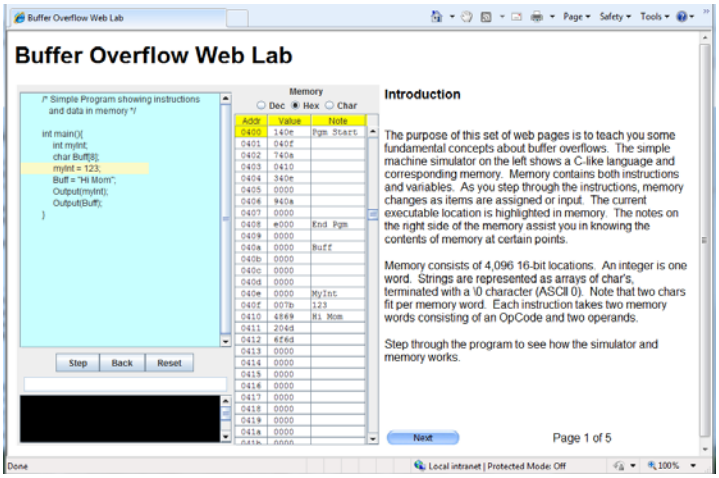

Figure 1- Buffer Overflow Web Lab

While reinforcing concepts well, a potential downfall of the web lab is in the accuracy of the simulation. Students may learn concepts well, but the transference of these concepts to a real life scenario has not yet been evaluated. Furthermore, the creation of the web lab requires a skilled JAVA programmer to create and test the program prior to usage in the classroom. The amount of time to create a comprehensive web lab is not insignificant.

ISBN 1-933510-96-X/$15.00

III. Our Approach

The Department of Computer Science at our institution has been teaching Information Security since 1996. Since that time, we have developed a variety of security curricula, tried numerous approaches to teaching specific concepts in the classroom, employed active learning techniques, developed hands-on labs, and participated in several security competitions. Since 2005, our institution has been recognized as a Center of Academic Excellence in Information Assurance Education. Our department currently has over 110 Computer Science Majors of which over 80 percent have chosen our Information Warfare option which includes three elective courses: Cryptography, Network Security, and Computer Security and Information Warfare. Additionally, we have found ourselves tasked with presenting computer security topics to a number of non-major students as well as students from local high schools and universities.

As previously mentioned, we use a laboratory component in our security courses to provide our students the advantages of hands-on experiences. Our lab has evolved over the years from a very traditional lab environment which included physical machines tied together on an Ethernet network. As we progressed to more complex security topics such as SQL Injection, Buffer Overflows and Firewalls, we discovered that our students were spending time trying to understand database, memory, and network topics instead of those objectives for which the labs were designed. Our solution to this was to begin using web labs. We use them to supplement more traditional lab experiences. More recently, we have begun using a VM approach for some of our labs.

IV. Concept Focused

In our experience, there is no single answer to the question of how best to implement a hands-on lab environment. In fact, it appears that a combination of traditional lab, web lab, and virtual lab environments in a single class may provide the best solution. One class in which we offer a multiple-lab type approach is our Computer Security/Information Warfare class. This class is at the undergraduate level offered as part of our Cyber Warfare option. The only pre-requisite to the class is basic networking. Although the class is primarily offered for Computer Science majors, it appeals to both Computer Engineering and System Engineering students as an elective. This variety of students in a single upper-level class has forced us to re-look at our lab environment to understand how concepts can be reinforced across the varied backgrounds of the students.

The class currently has a number of associated hands-on labs. These labs and their objectives are outlined in Table 1. It is clear from the lab objectives that the goal of each of the labs is to expose the student to the associated concepts in a way that they can understand the educational concepts associated with the subject. For example, the Firewall lab should expose the student to the basic concepts associated with how firewalls work and how firewalls can stop certain types of attacks, but there is no need for students to understand how specific firewalls work nor the details required to watch network traffic flow through a firewall trying to judge the success or failure of the firewall configuration.

Table 1- Information Warfare Lab and Objectives

Lab Subject	Objectives
Password Cracking	Know the attack strategies and countermeasures against passwords Understand the use of hashed passwords and purpose of salting
SQL Injection	Understand how databases work on a client-server environment and the role of SQL Understand defenses against Client and Server-Side attacks
Buffer Overflow	Understand the basics of buffer overflows, what causes them and how they can be exploited Understand the exploit of stack smashing to insert and execute code in a stack
Firewall	Understand the applications and limitations of firewalls Understand the role of rules in packet filter firewalls Know the type of information stored in a stateful inspection firewall and understand its advantage over a packet filter firewall
Vulnerability Exercise	Recognize and explain the relationship of increased tool complexity and reduced hacker technical abilities
Take-Grant Protection Model	Understand the purpose of the Take Grant Protection Model Be able to construct a Take Grant graph that represents a given protection state Know the four rules associated with Take Grant and be able to apply them to a graph Be able to use the Take Grant application to demonstrate whether a given subject can get access over a given object
HRU Security Model	Understand the purpose and basic concepts of the HRU model Be able to define and execute commands in the HRU model Be able to use the HRU tool to build a model and execute it

As our Information Warfare class evolved, we discovered as we focused on the concept which we wish to teach, the manner in which to teach the hands-on lab came out of a relationship of complexity and experience. This concept focused decision process is outlined in Figure 2. As illustrated, more complex topics or laboratory configurations presented themselves better with web labs while less complexity seems to lend themselves to virtual labs. The counterpoint to the complexity of the lab was the experience level of student and faculty lead. When faculty and/or students were highly experienced in a given topic, the virtual labs allowed us to provide more complex configurations for a hands-on experience.

ISBN 1-933510-96-X/$15.00

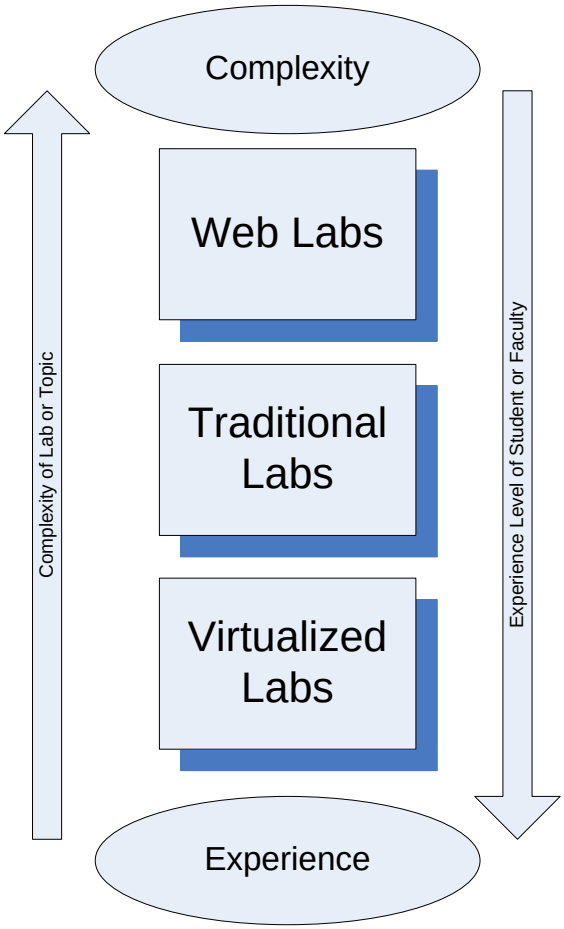

Figure 2 –Concept Focused Lab Choice Process

One way to explain this process in detail is to look at how our labs were created as hands-on, virtual, or web lab. Table 2 outlines the thought process behind the different choices made in our Information Warfare class. The Password Cracking lab, for example, has a low subject complexity and the associated laboratory necessary to meet the course objective was also low. This lends itself to a traditional lab in which students could use their own machines to attempt to crack passwords even when the student has a low level of experience. A subject such as SQL Injection, however, which required a more complex subject area (background in how databases work, how SQL is used, the concepts associated with client-server relationships, etc.), worked better with a web lab in which we could provide more detailed direction to the individual student while hiding the details of working with databases, networked environments, etc. While such a networked environment could be provided using a virtual lab environment, students with minimal background in networks and virtual machine usage seem to find a multi-system virtualized environment more difficult to understand than a web lab version of the same subject.

Table 2- Lab Choice Matrix

Subject	Complexity of Subject	Complexity of Lab	Experience of Student	Lab Choice
Password Cracking	Low	Low	Low-Medium	Traditional Lab
SQL Injection	Medium to High	High	Medium	Web Lab
Buffer Overflow	High	High	Medium	Web Lab
Firewall	Medium	High	Low to Medium	Web Lab
Vulnerability Exercise	Medium	Medium	Low to Medium	Virtual Lab
Take-Grant Protection Model	Medium	High	Medium	Web Lab
HRU Security Model	High	Medium	Medium	Web Lab

V. Conclusion

The use of concept focused labs offers the opportunity for instructors to choose an appropriate environment for hands-on labs based on a decision process focused on the subject material and the experience level of the student and faculty. Our experience is that a combination of all three lab types (traditional, virtual and web labs) allow us to focus on the concepts associated with the topic being covered when creating our labs. Complex subjects or lab configurations are best presented in a web lab environment in which we can control all aspects of the student's learning process, especially when the student's experience with the subject or networking environment is low. Highly knowledgeable students with a strong background in the subject or networking experience may find benefits in the virtual lab as they are able to conceptualize the multiple computer environment better. Subjects that are not as complex seem to fit best in a more traditional lab environment.

VI. Future Study

One area of future study is the ability of students to move concepts taught in web labs to a real-life scenario. Our web labs simulate complex topics such as buffer overflow or SQL injection yet we have no data on how well students transfer this experience to scenarios where they have to protect against such attacks. Additional web labs would be beneficial as well. One specific area in which we see benefits would be cross-site scripting (XSS).

Finally we feel that the creation of cross-course labs could be beneficial to permit the development of skills which cross more than one class. For example, the skills associated with networking cross into the domain of both our Computer Security/Information Warfare class as well as our network security class yet we have no cross-class labs to provide hands-on skill evaluation in this case. Creating such labs using the concept focused lab choice approach would benefit students of all three classes.

ISBN 1-933510-96-X/$15.00

VII. References

[1] "Computer Science Curriculum 2008: An Interium Revision of CS 2001." Retrieved March 2011, from www.acm.org/education/curricula/ComputerScience2008.pdf.

[2] Clinton, W. "Executive Order 13010-Critical Infrastructure Protection". *Federal Register*, 61, 138 (1996), 37347-37350.

[3] Office of the President (April 2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* US Government Printing Office.

[4] Irvine, C. E. (1999). *Amplifying security education in the laboratory* 1st World Conference in Information Security Education. Citeseer. 139-199.

[5] Crowley, E.(2004). Experiential learning and security lab design. In *Proceedings of the Proceedings of the 5th conference on Information technology education* (Salt Lake City, UT, USA, 2004). ACM.

[6] Vigna, G. "Teaching hands-on network security: Testbeds and live exercises". *Journal of Information Warfare*, 3, 2 (2003), 8-25.

[7] Du, W. and Wang, R. "SEED: A suite of instructional laboratories for computer security education". *Journal on Educational Resources in Computing (JERIC)*, 8, 1 (2008), 1-24.

[8] Pashel, B. A.(2006). Teaching students to hack: ethical implications in teaching students to hack at the university level. In *Proceedings of the Proceedings of the 3rd annual conference on Information security curriculum development* (Kennesaw, Georgia, 2006). ACM.

[9] Schweitzer, D., Gibson, D. and Collins, M. (2009). *Active Learning in the Security Classroom* System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on. 1-8.

[10] Abler, R., Contis, D., Grizzard, J. and Owen, H. "Georgia tech information security center hands-on network security laboratory". *IEEE Transactions on Education*, 49, 1 (2006), 82-87.

[11] Hill, J. M. D., Curtis A. Carver, J., Humphries, J. W. and Pooch, U. W. "Using an isolated network laboratory to teach advanced networks and security". *SIGCSE Bull.*, 33, 1 (2001), 36-40.

[12] Jensen, B., Cline, M. and Guynes, C. "Teaching the undergraduate CS information security course". *ACM SIGCSE Bulletin*, 38, 2 2006), 63.

[13] Schafer, J., Ragsdale, D. J., Surdu, J. R. and Carver, C. A.(2001). The IWAR range: a laboratory for undergraduate information assurance education. In *Proceedings of the Proceedings of the sixth annual CCSC northeastern conference on The journal of computing in small colleges* (Middlebury, Vermont, United States, 2001). Consortium for Computing Sciences in Colleges.

[14] Parmelee, R. P., Peterson, T. I., Tillman, C. C. and Hatfield, D. J. "Virtual storage and virtual machine concepts". *Ibm Systems Journal*, 11, 2 1972), 99-130.

[15] Bullers, W. I., Burd, S. and Seazzu, A. F. "Virtual machines-an idea whose time has returned: application to network, security, and database courses". *SIGCSE BULLETIN*, 38, 1 (2006), 102.

[16] Wu, Y. A. "Benefits of virtualization in security lab design". *ACM Inroads*, 1, 4 (2010), 38-42.

[17] Stewart, K. E., Humphries, J. W. and Andel, T. R. (2009). *Developing a virtualization platform for courses in networking, systems administration and cyber security education*. Society for Computer Simulation International. 1-7.

[18] Sun, W., Katta, V., Krishna, K. and Sekar, R.(2008). V-NetLab: an approach for realizing logically isolated networks for security experiments. In *Proceedings of the Proceedings of the conference on Cyber security experimentation and test* (San Jose, CA, 2008). USENIX Association.

[19] Wang, X., Hembroff, G. C. and Yedica, R.(2010). Using VMware VCenter lab manager in undergraduate education for system administration and network security. In *Proceedings of the Proceedings of the 2010 ACM conference on Information technology education* (Midland, Michigan, USA, 2010). ACM.

[20] Choi, Y. B., Lim, S. and Oh, T. H.(2010). Feasibility of virtual security laboratory for three-tiered distance education. In *Proceedings of the Proceedings of the 2010 ACM conference on Information technology education* (Midland, Michigan, USA, 2010). ACM.

[21] Anderson, B. R., Joines, A. K. and Daniels, T. E. "Xen worlds: leveraging virtualization in distance education". *SIGCSE Bull.*, 41, 3 (2009), 293-297.

[22] Border, C. "The development and deployment of a multi-user, remote access virtualization system for networking, security, and system administration classes". *SIGCSE Bull.*, 39, 1 (2007), 576-580.

ISBN 1-933510-96-X/$15.00

[23] Ketel, M.(2010). A virtualized environment for teaching IT/CS laboratories. In *Proceedings of the Proceedings of the 48th Annual Southeast Regional Conference* (Oxford, Mississippi, 2010). ACM.

[24] Schweitzer, D. and Boleng, J. "Designing web labs for teaching security concepts". *J. Comput. Small Coll.*, 25, 2 (2009), 39-45.

ISBN 1-933510-96-X/$15.00