Building a Vulnerability Testing Lab in an Educational Environment

Austin Whipple, Bishop Fox

Austin Whipple received a B.S. in Information Technology from BYU in 2014, where he led and worked on the Red Team. He now works as a Senior Security Analyst at Bishop Fox.

Mr. Keith B Smith, Brigham Young University

Keith Smith earned his Bachelors of Science in Information Technology at Brigham Young University with an emphasis in Information Assurance and Cyber Security. His educational interests lie in web application security and promoting cyber security awareness. Keith is married with three children. He currently lives in Redmond, WA,where he works as a Service Engineer for Microsoft.

Dr. Dale C Rowe, Brigham Young University

Dr. Rowe has worked for nearly two decades in security and network architecture with a variety of industries in international companies. He has provided secure enterprise architecture on both military and commercial satellite communications systems. He has also advised and trained both national and international governments on cyber-security. Since joining Brigham Young University in 2010, he has designed a variety of courses on information assurance, cybersecurity, penetration testing, cyber forensics, malware analysis and systems administration and published over a dozen papers in cybersecurity.

Samuel Moses, Brigham Young University

Samuel Moses is a research assistant and lab manager at Brigham Young University in the Cyber Security Research Lab. He is graduating with a Bachelors in Information Technology this year, emphasizing in the fields of System Administration and Cyber Security. After graduation, Samuel Moses is planning on continuing his education at Brigham Young University studying for a Masters in Technology emphasis in Cyber Security.

Building a Vulnerability Testing Lab in an Educational Environment

Introduction

In 2011, the Assistant Director of the FBI's Cyber Division, Gordon Snow, testified before a U.S. Senate subcommittee and predicted that, "The threat [cybersecurity] has reached the point that given enough time, motivation, and funding, a determined adversary will likely be able to penetrate any system that is accessible directly from the Internet." [1]

This has already been happening. In the last year (2014), it has been seen in mainstream media with the Sony Hack, Heartbleed, POODLE, and shellshock [2–5]. With so many prevalent examples, everyone has heard of at least one. This reinforces the idea that still today there is the need for more competent InfoSec professionals. The demand will continue to grow. InfoSec positions are projected to grow 37 percent, and it is growing much faster than average occupations [6].

To compound the problem, there is consensus among government officials, the private sector, and educators that there is a massive shortage of skilled cyber-security professionals[7–10]. This document proposes a fully-implementable program that addresses the growing need for cyber-security professionals. Research begins with identification of common roadblocks to implementing a cyber-security program. Next, this document discusses solutions to these obstacles. Finally, a detailed description of the program implemented at Brigham Young University is given, along with the results that have come from successful implementation. This work is a natural progression from previous attempts at solving this problem[11–13].

The Current Problem

Developing a successful educational program to train those interested in developing the cyber-security skill set is difficult. Most institutions interested in these programs must deal with limited resources when designing an appropriate learning environment, limited teacher time to devote to maintaining systems, limited administrative support due to misunderstanding of these skills, and accidental (or deliberate) misuse of tools and skills. All of these issues can hinder or halt a growing cyber-security program. These problems often lead to a program focused on theory with too little attention given to development of practical skills necessary for professionals.

Limited Resources

Without large or already-established budgets for developing a cyber-security program, the greatest obstacle to creating a good lab can be lack of equipment and software. Teachers may have limited server resources or, worse, just a handful of old, standalone computers. Additionally, some security software may be prohibitively expensive.

Limited Teacher Time

With teaching, researching, writing, and grading, teachers have finite time to personally mentor all interested students and maintain complex cyber-security virtual systems. Out of necessity, teacher time is often focused more on students who are struggling and need help. This can create a situation where some students are unable to benefit from the advanced techniques and knowledge a teacher possesses.

Limited Administrator Support and Understanding

Another obstacle that can come, often unexpectedly, is lack of department or school support, or even opposition. This is often due to misinformation, confusion over terminology, or lack of education on the subject of security and the need for InfoSec careers. Typically, these concerns range from a benign concern about lack of research possibilities to outright mistrust of students' self-control or competence with dangerous knowledge or tools.

Misused or Misdirected Tools

Perhaps the biggest danger to the institution as a whole is misused or misdirected tools. If a tool is left running after being used, or pointed at the wrong network, it could mean loss of data or downtime for innocent servers. If malware is improperly isolated in a testing environment, it could easily escape and spread inside a well-connected campus. Additionally, other students may become accidental (or purposeful) targets of malicious students.

Proposed Solutions

This section details solutions to each of the problems mentioned in the previous section. The reader is advised to keep in mind that many of these solutions assume that students are interested in contributing to a learning environment, instead of abusing the system. The solutions detailed are in agreement with what was observed from students using the system created for this research.

Limited Resources

To address limited resources, the researchers decided to leverage open-source and free software available to universities. For educational institutions, Microsoft and VMware products may already be offered free or at academic costs. At the time of this writing, educators can obtain a free license for VMware vSphere through their academic program using an ".edu" email address. Combined with a free copy of ESXi, educators can use virtualization to build an entire network with very little hardware. Using virtual machines with Linux and Windows brings the cost of software down to nothing.

Additionally, surplus computers work well as hosts for vulnerable configurations, as they typically only need to be attacked and do not need to serve with a great degree of reliability or speed. Most educational institutions that have plentiful surplus machines as computer labs are upgraded. Often these surplus machines can be saved to be used as a vulnerable machine.

While many companies will argue that they have the best security tools for performing tasks, the skills required to use these tools can be learned using readily available open-source tools found in penetration testing distributions such as BackTrack and Kali Linux [14].

Limited Teacher Time

Since teachers will likely not have the time to create or upgrade a security program single-handedly, hiring a research assistant to perform initial infrastructure setup may be an option, after all stakeholders have agreed on the policies that should be in place. Research assistants may put ESXi on a server with ample hard drive space, assign subnets, put vSphere on the server, and use VMware Standalone Converter to begin uploading VMs.

For teaching the students to hack the VMs, there are plenty of videos and walkthroughs on the web to guide a student on most of the vulnerable VMs. Teachers and assistants can fill a support role when needed and provide mentoring to students who work on these often difficult problems. This builds expertise and experience. Students can be reminded that hacker culture was spawned by thinking outside the box and using technology to do things it was not designed to do.

The environment this develops sets up the opportunity for student leadership and growth, while also increasing available teacher time. With different organizations being created as side benefits, students can take charge and run these organizations. Using these organizations as an education platform, students can learn, provide a service, and share knowledge and experience with one another. With students leading, the teacher's main duty is mentoring and advisement. The teacher's role here prepares the students to help teach other students as well.

The system that this paper will describe naturally creates an environment where those willing to invest the most time rise to the top. However, this system can also, if misused, create an environment of laziness and over-reliance by teachers. The best way for teachers to counter this is to be actively involved in both teaching the students and facilitating hacking activities.

Limited Administrator Support and Understanding

In response to limited administrator support, it was found beneficial to provide monthly "current ethics" lectures. During these lectures, a faculty advisor, an experienced student, or a guest speaker talked about current events related to ethical hacking. This group meeting can be other things in addition, but it will show due diligence in informing students that they can use their skills to benefit society instead of ending up in jail. When addressed correctly, penetration testing and other cyber-security activities provide a strong background for developing ethics and integrity in individuals [15,16].

Additional reassurances may require making the vulnerable lab available only to students who participate in these meetings and sign a form indicating their agreement to not use the tools in an unauthorized manner. At BYU, consequences of breaking this agreement include being unable to participate in activities and their activity being reported to the Honor Code office, which handles ethical concerns.

Limited understanding can be addressed by allowing students obtaining security knowledge to do presentations to campus, local systems administrators, local schools, and businesses. Students take the lead in educational outreaches where they can teach others the basics of security. This allows students to gain valuable real-world experience that sets them apart from their peers and educates the community.

With administrators coming from different backgrounds, both technical and non-technical professionals, terms can cause different meanings and context. For example, the term hacking can sometimes have a negative connotation. Within this last year there has been the Sony hack, and celebrity photos being stolen, as well as massive attacks against retailers causing loss of credit-card data which is what most people think of with the term hacking. This is not how InfoSec professionals use the term though. Hacking describes when someone changes something to use it for what it is not its original intended purpose. Teaching and explaining the meaning and context behind these terms to administration can help them make better and more informed decisions when it comes to a cybersecurity program.

Misused or Misdirected Tools

One objection that will come up regards the wisdom of putting a set of purposely vulnerable computers on the network and allowing students to use potentially dangerous tools on that network. This can easily be avoided by assigning one subnet to the victim machines and one subnet to the attacker machines on a routed network. After it is segmented, the entire vulnerable network can be separated from the rest of the network with a student accessible Ethernet cord that can be unplugged. Students know that the cable must come out once tools start going over the wire. For students using their own machine as the hacking machine, wireless connectivity should be disabled during any exercise. For additional security, put an IDS/IPS/firewall outside of the gateway to the network. The firewall can be used to disallow non-management traffic coming into and out of the network.

A malicious student is something that is harder to defend against. With the skills and tools being taught to these students, it is important that they understand the laws and ethical implications of their actions. This is why when working with students at BYU, the laws and ethical situations they might run into are always brought up and discussed. Furthermore, all students are required to sign a code of ethics so they understand their responsibilities completely. Then in many of the engagements that they might be involved in, there is often a Non-Disclosure Agreement (NDA) that they are required to sign. Even with all these legal protections, it is necessary for the teacher to be able to trust his or her students. It is important that anyone reports anything that might be suspicious that they run into. This makes the responsibility of keeping the vulnerable lab an ethical environment the duty of both the students and the teacher.

Existing Solutions

There have been other solutions that have been created to help address the shortage of InfoSec professionals, like the National Collegiate Cyber Defense Competition [17,18], (NCCDC), CyberQuests, and CyberDefense. These solutions have been helpful with the shortage, but do not address it in an early enough manner to help.

The mission of NCCDC is to provide institutions that have a cybersecurity curriculum a controlled, competitive environment to test and assess students' technical understanding and operation competency by completing challenges designed to mock realistic scenarios involved in protecting a network infrastructure and business systems[17] (see also http://www.nationalccdc.org). The NCCDC is a good testing ground, but does not lend itself to a teaching environment. Students are able to learn much about their teamwork skills and see how they react in real world environments, but the competition is very fast pace. This does not allow it to be a learning environment, but rather a testing environment for students who have already learned the skills.

CyberQuest is a series of online challenges allowing participants to demonstrate their knowledge in a variety of Cyber Security areas (http://uscc.cyberquests.org). Each challenge features a different aspect of cyber security with a series of questions to go along with it. The challenges have a variety of difficulties and complexities with some challenges having material better fit for beginners and others geared for intermediate and advanced. CyberQuest's challenges and quizzes are helpful for students and InfoSec professionals both, but again expect those participating to be qualified and trained to understand the challenges more than being a starting ground to begin training.

The existing solutions are helpful in testing one's understanding and operational competency, but are not the best learning environment. The lab in this paper is a better starting ground to help prepare students to the point where they can participate fully in these existing solutions.

Full Solution Configuration and Setup

For the vulnerable lab used at BYU, Cyber Security Research Lab (CSRL) designers used surplus hardware, free software, free training material, and a small web server for student resources. This section provides valuable advice for getting the vulnerable lab set up and configured to support vulnerable OS distributions available online.

Hardware and Software Setup

For BYU's setup, the team used ESXi on a number of blade servers, all behind a virtualized vSphere Server. Each server connected to a SAN used to store machine images. To upload vulnerable machines, researchers used vConverter to convert machines to ESXi compatible images. vSphere client was used to manage stored images. The vSphere client can be configured to allow students to have a limited-privilege account. This allows students to bring machines up or reset them. A Vulnerable Lab Administrator can also be tasked to maintain and add to the machines. Each software tool described here is a free educational license obtained through VMware's academic program. All hardware used in this configuration was several-year-old surplus obtained from BYU.

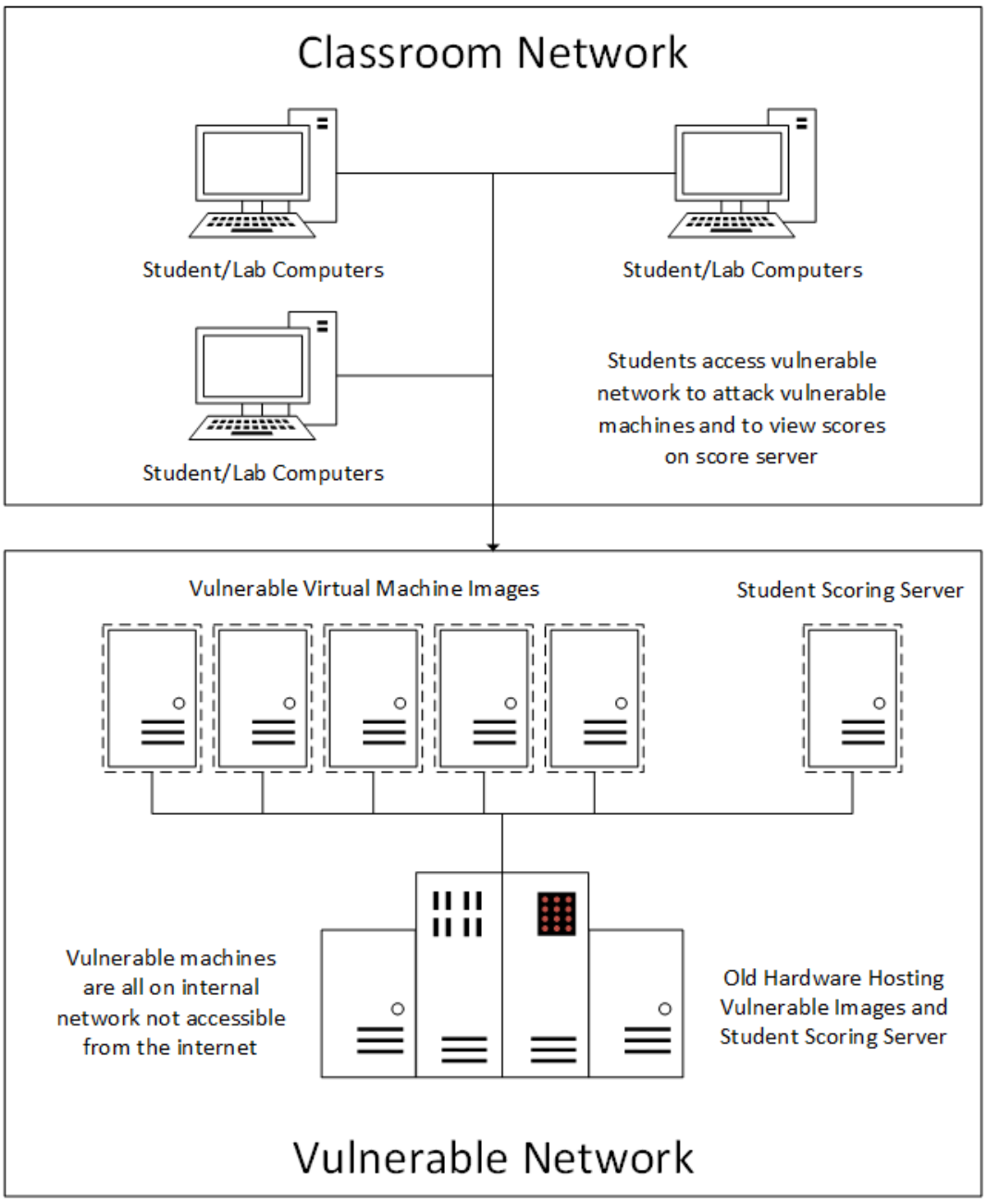

Figure 1: Vulnerable Testing Lab diagram.

Virtual Machine Setup

The first issue we encountered was getting the virtual images on our ESX server. Most of them did not have an issue once we put them up, but some refused to boot. The next obstacle when dealing with pre-built open-source vulnerable virtual machines is logging into these machines. Since these are often presented as challenges with little or no information given, users are not typically given valid login credentials. To obtain valid credentials, often a walkthrough already exists that provides credentials or a valid solution. When a walkthrough is not available, the vulnerable machine can usually be booted into single-user mode to reset root administrative

credentials. If single-user mode fails, it is frequently possible to boot into a LiveCD like Knoppix, mount the vulnerable machine, and change the password hashes to a known value that can be used to login.

Once valid login credentials have been obtained, the next step is to start changing configuration settings on the machine. Changing passwords will prevent students from bypassing machines by using walkthroughs found online. Depending on the experience level of those administering the lab configuration, it might also be possible to reconfigure vulnerable machines to be vulnerable in a slightly different manner than the original author intended. When doing this, it is very important to give credit to the original author with any derivation of a work. Next, it is important to delete or change permissions for the DHCP executable to prevent IP addresses from being reassigned. In the BYU Cyber Security Research Lab (CSRL) setup, each IP address was set to a static IP. A listing of the IP address of each machine was documented for later use.

For quick grading purposes and for using this system competitively, creating a "flag" file on each machine can provide students with proof that they have hacked the vulnerable machine. The "flag" is a file that contains a phrase or value that provides conclusive evidence that the flag file was obtained from the system. This file is generally stored in the root directory, which requires root access to the system to read. In the CSRL system, a web interface was created that allows for flag submission and scoring.

Once the set-up of each machine and its networking components is completed, a snapshot of each machine in the CSRL setup was created. The snapshot provides a method for easy backup and a method of rolling back corrupted images to the correct state. Now the machines are allowed to be compromised many times by students and still maintain a consistent state.

Web Server Setup

As briefly mentioned above, a major contribution to the success of the setup is a simple web server whose IP address lies outside of the allowed IP scope for attacking. The web server provides a scoring engine to students and teachers. Students that are able to compromise vulnerable machines can submit flags obtained for points on this engine. This naturally creates a leaderboard where teachers can gauge the progress of students. Students are provided with feedback on their progress and a means of comparison with peers. To facilitate this, the CSRL team used a free scoreboard engine that was previously used as a hacking CTF (Capture The Flag) scoreboard.

This web server can also be used by students to submit write-ups of their solutions that other students can use if they are stuck. These can be reviewed by the TA/RA and posted for the group members to see, and provide another method for teachers to see who is most interested and willing to contribute to the community. As this web server is used, it becomes a valuable knowledge base of security resources available to students and teachers for increasing the effectiveness of InfoSec programs.

Benefits

After having built this lab, CSRL lab designers have noticed a number of side benefits naturally occurring from the creation of this system.

Cyber Security Students Academic Association

Attracting students interested in security has led to the organization of a Cybersecurity Club. The club provides training, regular tech-talks and events such as capture-the-flag competitions. Also, interested students get directed to a Cyber Security Research Lab (CSRL). The CSRL consists of interested security students and professors working together on several research projects involving security. This research group extends the benefits of training security professionals by producing original content that is valuable to the security field.

Red/Blue Team

In addition to the benefits described above, the CSRL at BYU currently manages the school's Red and Blue Teams[5] which provide valuable penetration testing and incident response resources to X and local businesses. To support these efforts, the CSRL is able to utilize the lab to better hone these teams' skills in mock penetration tests. Systems can quickly be built that host similar vulnerabilities found in team engagements in order to identify ways to fix or mitigate security problems.

Future Work

With the success that CSRL has had with this initiative, the research team plans to do a number of things to augment the system. As additional vulnerable machines are authored and released for public consumption, plans have been made to add them to the vulnerable network as resources permit. As students become more proficient with the tools and techniques necessary to compromise vulnerable machines, these students will be able to expand upon these machines and create their own vulnerable testing machines. These will be given to the open-source community and added to the network for future use.

To further improve the vulnerable lab, the team plans on categorizing the different machines in the vulnerable network. This will allow for the creation of structured learning paths and curriculum that can be used to teach specific skills and techniques. The web server can be converted to a valuable tool that will provide a means for helping students learn by specific topic.

Conclusion

Higher education programs that follow and adapt these guidelines will create a system that provides low-cost, high-benefit solutions central to organizing a strong cyber-security program. The solutions that have been outlined produce a state-of-the-art cyber-security program at any institution, providing students with real, applicable cyber-security skills. This system can also be easily modified or expanded as needed to meet individual needs for each institution, addressing the worldwide need for qualified cyber-security professionals.

Bibliography

1. Snow GM. Cybersecurity: Responding to the Threat of Cyber Crime and Terrorism. 2011.

2. Redhat Customer Portal. How to recover from the Heartbleed OpenSSL Vulnerability. RedHat. 2014 [accessed 2015 Jan 12]. https://access.redhat.com/articles/786463?sc_cid=70160000000d4tGAAQ

3. Redhat Customer Portal. POODLE: SSLv3 Vulnerability (CVE-2015-3566). RedHat. 2015 [accessed 2015 Jan 12]. https://access.redhat.com/articles/1232123?sc_cid=70160000000eITIAA2&

4. Trend Micro. Shellshock BASH Bug Exploit. Trend Micro. 2015 [accessed 2015 Jan 12]. http://www.trendmicro.com/us/security/shellshock-bash-bug-exploit/

5. McCain J. America must fix it's cyber-vulnerability. CNN Opinion. 2014 [accessed 2015 Jan 12]. http://www.cnn.com/2014/12/20/opinion/mccain-cyber-attacks/

6. US Department of Labor - Bureau of Labor Statistics. Information Security Analysts. 2014.

7. Adams WJ, Gavas E, Lacey T, Leblanc SP. Collective Views of the NSA/CSS Cyber Defense Exercise on Curricula and Learning Objectives. In: Proceedings of the 2nd Conference on Cyber Security Experimentation and Test (CSET'09). Montreal, Canada: USENIX Association; 2009. p. 2. http://dl.acm.org/citation.cfm?id=1855481.1855483

8. Beidel E, Magnuson S. Government, military face severe shortage of cybersecurity experts. National Defense. 2011;96(693):32–34.

9. Booz Allen Hamilton. Cyber In-Security: Strengthening the Federal Cybersecurity Workforce. 2009.

10. Obama B. Remarks by the President on Securing out Nations Infrastructure. Office of the Press Secretary, The White House. 2009.

11. Bursztein E, Gourdin B, Fabry C, Bau J, Rydstedt G, Bojinov H, Boneh D, Mitchell JC. Webseclab Security Education Workbench. In: Proceedings of the 3rd International Conference on Cyber Security Experimentation and Test (CSET'10). Washington DC: USENIX Association; 2010. p. 1–9. http://dl.acm.org/citation.cfm?id=1924551.1924558

12. Fanelli RL, O, Connor TJ. Experiences with Practice-focused Undergraduate Security Education. In: Proceedings of the 3rd International Conference on Cyber Security Experimentation and Test (CSET'10). Washington DC: USENIX Association; 2010. p. 1–8. http://dl.acm.org/citation.cfm?id=1924551.1924555

13. Vigna G. Teaching Hands-On Network Security: Testbeds and Live Exercises. Journal of Information Warfare. 2003;2:8–24.

14. Kercher KE, Rowe DC. Risks, Rewards and Raising Awareness: Training a Cyber Workforce Using Student Red Teams. In: Proceedings of the 13th annual conference on Information Technology Education - SIGITE '12. New York, New York, USA: ACM Press; 2012. p. 75–80. http://dl.acm.org/citation.cfm?id=2380552.2380573

15. Dark M. Using Educational Theory and Moral Psychology to Inform the Teaching of Ethics in Computing. In: InfoSecCD '05 Proceedings of the 2nd Annual Conference on Information Security Curriculum Development. New York, New York, USA: Association for Computing Machinery (ACM); 2005. p. 27–31.

16. Dark MJ, Epstein R, Morales L, Countermine T, Yuan Q, Ali M, Rose M, Harter N. A Framework for Information Security Ethics. 10th Colloquium for Information Systems Security Education. 2006.

17. White GB, Williams D. The National Collegiate Cyber Defense Competition. Tenth Colloquium for Information Systems Security Education. 2006.

18. White GB, Williams D. Collegiate Cyber Defense Competitions. Ninth Colloquium for Information Systems Security Education. 2005.