Real-World Security Lab Environment

Ben Eckart, *Manhattan Area Technical College, Manhattan, Kansas*

Abstract – We all know that it is necessary for educators to provide their security students hands-on experiences. Without these experiences students are not going to be prepared for the world of work, where employers expect the graduates to hit the ground running. To address this issue many different approaches have been used, such as traditional labs, virtual labs, and simulated web labs. Similar to other institutions, we have used all these approaches with high levels of success. However, because our students are expected to have real-world experience, our college has moved most, if not all, of the final semester hands-on labs to real-world, live Internet labs. This paper describes our decision processes for converting our labs to this real-world approach and our experiences in that environment.

Index terms – Real-world scenario lab, live lab, security, real-life scenario lab, Internet connected lab, security curriculum, network security laboratory, information security laboratory

I. INTRODUCTION

In the information security area, live labs can sometimes pose unique challenges. In a recent paper there was a discussion about different approaches to security labs that focused on traditional labs, virtual labs, and simulated web labs. The discussion revolved around the benefits of each approach and the processes used to decide which approach would be best in different situations. At the end of the paper under the heading "Future Study" was a challenge to move concepts taught in web labs to a real-life scenarios [1]. We have been dealing with this challenge for many years and believe we have had great success with our real-life scenario labs. The use of isolated lab environments, where hands-on experience is performed in a sterile and isolated network without outside connectivity, has been an ongoing frustration. With the need to protect the institution's network there is a fear about letting our students experience that real world. Those fears are well-grounded because all instructors have horror stories about a networking class using duplicate IP addresses, wrong domain name service (DNS) server settings, improperly configured routers, and numerous other novice mistakes that result in a call from the Information Technology (IT) Department and possible restrictions on, or loss of, outside connectivity for the Networking and Security Department. Without an understanding of the consequences of misconfigured network devices there are numerous ways for lab errors to occur.

With this in mind we still believe that live labs are an important part of preparing students for the real world. The question then is, "How can this be done while still protecting the campus network and not experiencing the wrath of the IT department?" Also, what decision processes should be used to determine which labs could be converted to this approach? Recognizing that not all school IT departments are alike, some working relationships are necessary in order to be successful using this real-world approach. These factors will be addressed along with some of the problems that can be encountered, as well as solutions for these problems.

The educational ideal would be for students to experience all the problems they would encounter if applying the same solution on the job. In newly published lab manuals and lab resources developed for security, the authors want to provide an environment for students to "try out" tools and skills with limited or no risk to the campus network. By doing this they "protect" students from accidently damaging systems, resulting in serious consequences. In one paper the authors listed eight general principles that guide the design of an information security laboratory, among which was "Realistic and Isolated" [2]. How can we have isolation without sacrificing realism? This design also used controlled student servers and workstations that did not allow them to make changes to these machines. This begs a question about how students can experience malware, viruses, and security issues if nothing can be changed. Service packs, updates to operating systems, virus protection software, and malware

ISBN 1-933510-95-1/$15.00

signatures will not be part of their realistic experience.

Another design took a distributed lab approach. These labs are connected to the real world through their own Internet connection, separate from the campus network, providing isolated but connected labs. However, this method does not give the lab real Internet access but, rather, gives secure access to other campus labs, even at other schools, but does provide a wide range of opportunities. This lab does have provisions set up so students can have access to, and download from, the Internet, but only from select workstations [3].

II. OUR EXPERIENCE

Our labs have evolved over the years and, as resources were made available, the labs became more complex. All workstation and server operating system labs have always required Internet access so we can teach updating, spyware protection, and virus protection. When they enter the program students are issued a workstation/server machine and are required to purchase a laptop computer, which acts as another workstation. They are also given a unique range of private IP addresses to use for their labs, which they maintain until program completion.

When networking became the main focus we started with an isolated lab environment, but soon realized we were protecting the students from getting a complete experience, so we connected them to the college's network and the phone started to ring. In order to continue we had to isolate our students while maintaining the real-world connection; therefore, we installed our first router between the department and the college's network, which solved all but the most complex problems. The router did created problems that needed to be solved, such as our own private network needing its own dynamic host configuration protocol (DHCP) and network address translation (NAT) services.

As our focus evolved to more information security training, other issues arose. One of the biggest is that the IT department blocks most of the services we need for security labs. The other thing the IT department does is web filtering to protect the network, which blocks most of the research and security download sites. Our solution to these problems was to get our connection to the Internet to bypass the firewall and filter rules imposed on the rest of the campus. With our great working relationship with the IT staff we were able to make this possible. That put the responsibility for those services on the shoulders of the networking students and faculty. This actually presents an opportunity to use what they know (e.g., DHCP servers, DNS servers, and NATing).

Because of college policy changes, labs that worked one semester would fail the next. Also, changes made to the college's network or Internet provider might affect things like gateway and DNS values. Without good communication with the IT staff these changes could cause delays in students completing labs affected by the changes; however, we were able to solve these problems.

Where are we now? Currently we have a situation where we do not touch the college's Internet connection at all. We have private connections to the Internet for the Information & Network Technology (INT) Department, but this presented its own problems. One being that, in the past, if we had an Internet connectivity problem we contacted our in-house IT staff and it was taken care of. Now we have to deal directly with the Internet provider, which is also a real-world experience and another opportunity for our students to learn.

III. REQUIREMENTS

So which labs are candidates for conversion to real-world labs? The best answer is all of them. When the graduates get jobs they rarely work in an isolated network. So our belief is that they should be connected to the real world when doing all labs. The one exception might be basic routing labs, but these too could be done in the real-world lab environment as long as caution is taken. The process we went through was to take existing labs and develop the steps necessary to make them live.

So what steps are necessary to make the labs work live without interrupting the campus network? Most of the steps are taught in advanced networking and security classes so, as our students move through our program, the knowledge needed for using the live environment is acquired.

IV. EXAMPLES

The following are some of the ways this is working for us.

ISBN 1-933510-95-1/$15.00

A. Secure Electronic Commerce (eCommerce)

Teaching students about public key exchange, digital certificates, trusted networks, and cryptography, is pretty straightforward using examples and some basic labs. However, experiencing how to secure a real eCommerce site would first require a web-facing eCommerce site. This might seem like a major undertaking but it is not. There is really only one major fear using these temporary web sites and that is, with current search engines, outsiders will find these sites, which may appear legitimate, in sometimes less than a few hours and, and at the least, that would cause confusion and, at the worst, individuals may try to actually purchase items from the site. There are no penetration tests or scans done from these sites.

In a lab series we developed, students, either through physical servers or virtual servers, build an open source eCommerce site that is a catalog of make-believe items. They observe that it is an unsecured site (i.e., the lock in the browser is open). They also capture a transaction and see that the packets are in plain text and readable. Next they secure the site with a trial secure sockets layer/transport layer security (SSL/TLS) certificate from a well-known third party certificate authority. When that is done, the captured transaction is encrypted and unreadable. They now have a secure site as observed by the closed lock in the browser. Currently we are working on adding the Extended Validation (EV) SSL/TLS certificate to the lab, as identified by the green highlight in the browser's address bar.

We have had great success with this lab and the students can usually complete the installation of the certificate in less than an hour. In our capstone class they actually purchase an annual certificate and it is renewed each year. If it would be preferential for students to not use trial certificates, annual certificates can be purchased for around $75 per year and reissued as many times as needed. Also, this lab is done using both Windows and Linux operating systems.

Vulnerability testing can now be done from within the security lab, which is the same subnet as the web server. In this way the testing traffic does not leave the network.

The only major service that must be provided to the students is web-facing DNS—through the campus IT DNS server, the department's web-facing server, or the domain name registrar.

B. Live web server

Most schools have a basic web development or hypertext markup language (HTML) class in which students learn to build web pages, and server classes usually have a lesson and a lab on how to build a web server. We have taken that a step further by securing the web site with a real SSL/TLS certificate. Using the same or a new certificate from a third party certificate authority, they can change the web page transfers to secure encrypted transfers and can be observed using the same packet capture method on which they have been trained. The EV certificate could also be used and the same testing that is done in the secure eCommerce lab can be done here.

Another observation we have made is that it is easier to explain the way certificates work when we have a real certificate with which to work. Since it is owned by the college, it can be broken and used with these cases as a way to teach students how to troubleshoot certificate problems. We have had great success with this lab and it can take less than 15minutes if the student has previously built a web server and either has it saved or can rebuild it quickly.

C. Network security hands-on final

Securing network devices is important, but letting students connect routers to the live network can cause numerous problems. One of which is that, if improperly configured, it can bring down all connected networks.

We have developed a network security hands-on final where students must first configure a firewall to connect to the Internet and then check for and mitigate vulnerabilities on a router, network switch, and a server. We check the firewall configuration step first to ensure they have correctly completed the task before going on to vulnerability testing so the rest of the final can be completed without danger of causing problems with the network or other students. The rest of the final consists of finding vulnerabilities on different network devices we have connected. This is where the Internet connection is so important. They do not know which vulnerability they will find and must research a solution via the Internet. Once they have found a solution it sometimes requires them to download a patch, updated signatures, or software applications to correct the vulnerability.

Final tests are made to ensure they have corrected the identified problems and the vulnerabilities have been removed.

This too has been successful. Since the firewall is between the student's lab equipment and the Internet, bad packets are not released through the firewall so as to cause any negative effects. The biggest drawback to this process is that we can only test a couple of students at a time because the firewalls are costly.

D. Virtual labs

All of the above examples can be done on either physical or virtual server machines

V. CHALLENGES

As we have experienced and as noted by others [3], there exist many challenges in providing realistic network security laboratories. These are identified below:

A. Need to protect campus networks

The college IT staff has a duty to protect the campus network from security breaches, hacking, viruses, and malware. We cannot expect them to jeopardize the security and functionality of the campus network just so we can have our students do labs. I believe the first step in putting our method into practice is to establish a trusted relationship with the campus IT staff. Without this trust these techniques may never be able to work. Campus security policies, usage policies, or any other rules that maybe in place cannot be circumvented. As noted, the relationship with our IT department is great. There is complete trust between the network/security faculty and the campus IT staff. I have visited other schools where the exact opposite is true. Everything the faculty wants to do must be done in secret or by going over the heads of the campus IT staff, which only makes matters worse. Even with an independent Internet connection it is still necessary to have a firewall to protect against outside attacks.

The SANS Institute has published an Internal Lab Security Policy. This policy establishes information security requirements for labs to ensure that confidential information and technologies are not compromised, and production services and other interests are protected from lab activities [4]. SANS has also published a demilitarized zone (DMZ) Lab Security Policy that establishes information security requirements for all networks and equipment deployed in labs located on the DMZ. Adherence to these requirements minimizes the potential risk of damage to the public image caused by unauthorized use of resources and the loss of confidential data and intellectual property [5].

B. Need to access the Internet

Without direct connection to the Internet there is no way for students to correct the vulnerabilities they find, such as malware, security problems in the host operating system, or viruses. They need to be able to download updated signatures, operating system patches, and malware tools. Without this access they cannot conduct research on the tools needed to perform their job. Even Internet access through the campus backbone will not be sufficient because there will be rules and filters in place on firewalls to block these sites as malicious.

C. Difficult to simulate enterprise-/departmental-level network environment

In the real world, an enterprise or departmental network consists of a multitude of hardware and software devices. The task of installing, configuring, deploying, and maintaining such a complex network has proven to be a major challenge, especially for individual instructors who are interested in teaching computer security in a realistic enterprise network environment [3]. In order to address some of these issues, we have used upper level students to help maintain this equipment and we also have a lab assistant who is an enrolled student. As noted earlier, the services and equipment needed to maintain the hardware and software are taught in the networking classes.

Tikekar and Bacon [6] discuss the development of lab exercise levels—a beginning level that includes exercises that mirror an actual enterprise and allow machines to be "attacked" while protecting the campus and external networks, a second level that models real-world situations like finding vulnerabilities in a system and using them to gain access to the system, and a third level that has the students completing larger exercises or projects, which are undertaken at the capstone or graduate level. We use a similar approach but there is less distinction between the first and second levels except in terms of difficulty. We do have a capstone course that has up to six real IP addresses assigned and it is a

live real-world enterprise network with a main site, a remote office, and remote users. The course even has its own registered domain name and SSL certificate.

D. Difficulty in allocating various resources for different assignments

Budgets are always an issue and our college is no different. This can only be solved by being creative, frugal, and finding other sources of money. We buy as much as we can each year and there is some sharing of equipment. Varying lab schedules helps here. We also use donations and grants to supplement the regular budget. We have actually done pretty well with our budget and have been lucky in some ways.

E. Resources needed for students

Not all colleges require students to own portable computers; however, for over 20 years we have required the beginning students in our program to own a laptop computer. Also, we developed creative ways to purchase a physical server for each student, which he/she uses until exiting the program. These are then recycled to the next group of new students.

F. Easy and secure access to resources.

The resources available in the lab should be easily accessible. Students may choose to use the lab either locally or remotely (e.g., from home or from their workplace). Since our labs are directly connected to the Internet we can use any method available to give students access. We also use a virtual lab that is accessed via the Internet.

G. Incorporation of latest technologies

New technologies are constantly created. To accommodate the latest technological developments, such as wireless networking, secure remote access, etc., it is important that the design of the security lab be scalable. When we are able to purchase new technologies the older equipment is recycled to the lower-level classes where there are fewer requirements. The capstone class is the testing ground for designing, implementing, and documenting the new technologies through graded special research projects.

H. Ancillary duties required for configuring and maintaining the numerous lab devices

A dedicated lab assistant, if you can get one, is the best way to deal with lab maintenance; otherwise, student aides or even upper-level students may be used to assist the instructors in setting up lab projects and assignments. Also, saved configurations, the use of cloning, and virtual machines with the ability to take snapshots, as well as having base templates, make this job manageable.

I. Protecting students from each other.

As mentioned earlier, protecting students from one another can be a real problem, and we all have horror stories about a networking class using duplicate IP addresses, wrong DNS server settings, improperly configured routers, and numerous other novice mistakes. Since we are isolated from the campus network we are not injecting the problems there, but students can disrupt the lab network. We embrace this problem as an opportunity for some real network troubleshooting.

VI. NEEDS FOR IMPLEMENTATION

So what is needed to make this work? First, you need a connection to the Internet that is not filtered by the campus firewall. The preferred connection would be your department's own connection. The Internet service provider will give you at least one public IP address and more if needed. You will only need one public address for most labs.

The department will need a good firewall for the connection but without filtering. This firewall needs to be under the control of the department; however, if there is a good relationship with the campus IT staff they could configure and maintain it. If your department teaches firewalls then the faculty or lab assistant could maintain the firewall.

An Internet-facing DNS server is also needed. This could be done with an inexpensive Linux box that has DNS services configured, or it could be handled by the domain registrar. We teach DNS servers as part of our server classes so faculty or students can configure and maintain the servers.

An internal DNS server is also needed and the above solutions can work here except for the domain registrar.

Since SSL/TLS digital certificates work only with domain names and not IP addresses, you will need at least one registered public domain name. With a

single domain name you can have students use sub-domains, such as "studentname.yourdomain.com." We are currently working out a plan to have students register their own domains. With this approach students can use them for other labs, such as in web page design classes or just for personal use (e.g., posting a résumé). These personal domain names can be purchased for as little as $12 a year.

The rest of the resources, such as routers, switches, servers, and workstations, can be those already in the department, or you can use virtual machines for servers and workstations.

VII. CONCLUSION

One thing that should be noted is that this approach did not evolve over night. When we first started having students do labs we isolated them. When we tried to give them connection to the campus network things started to happen, and they were not good. We solved each of these issues and moved on. As more and better resources became available we expanded existing, and developed more, labs using this model. We are currently having great success and the students realize the real-world experience we provide has some challenges, but they are just like what would be experienced on the job. As our campus IT administrator always says when students ask him to help with a problem, "Welcome to my world."

VIII. REFERENCES

[1] Fulton, S. & Schweitzer, D. (2011). "A Concept Focused Security Lab Environment." *15th Colloquium for Information Systems Security Education, Fairborn, OH,* June 13-15.

[2] Padman, V. & Memon, N. (2002). "Design of a Virtual Laboratory for Information Assurance Education and Research." *Proceedings of the 2002 IEEE Workshop on Information Assurance and Security,* United States Military Academy, West Point, NY, June 17-19.

[3] Yang, T. A., Yue, K-B, Liaw, M., Collins, G.,T., Venkatraman, J.,, Achar, S., & Sadasivam , K., (2004). "Design of a Distributed Computer Security lab." *University of Houston-Clear Lake, Houston,TX* ,© 2004 by the Consortium for Computing Sciences in Colleges.

[4] SANS Institute (2006). Internal Lab Security Policy. Retrieved from http://www.sans.org/security-resources/policies/Internal_Lab_Security_Policy.pdf

[5] SANS Institute (2006). DMZ Lab Security Policy. Retrieved from http://www.sans.org/security-resources/policies/DMZ_Lab_Security_Policy.pdf

[6] Tikekar, R. & Bacon, T. (2003). The challenges of designing lab exercises for a curriculum in computer security. *The Journal of Computing in Small Colleges, 18*(5), 175-183.