ADDING WHEN, WHERE, AND WHY TO HOW

Providing Ethical Context in Aggressive Information Security Labs

Scott J. Roberts and Andrew L. Reifers

School of Information Sciences and Technology, Penn State University – University Park,

NSA Center for Information Assurance Excellence

Abstract Educators recognize that laboratory based computer security courses do far more for students' understanding than purely theoretical courses. Laboratories with common hacker tools are invaluable for students in an Information Assurance curriculum. These tools help students better understand threats and the defense mechanisms needed to protect individual systems and entire networks from these attacks. Students greatly benefit from understanding the threats they are called to defend against, making them more effective protectors of enterprise or government networks. Conversely these labs offer students hands on experience with tools that could easily be turned and used against others. Through the use of situations that show ethical uses of these techniques students can have these beneficial experiences without becoming the very danger they are being trained to protect against.

Key Words Information Assurance, Ethics, Laboratory Exercises

1. INTRODUCTION

With the growth of networked businesses and organizations many positive elements of society have branched out and begun to flourish into cyberspace. Commerce has fully embraced the Internet, and e-commerce is becoming more mainstream everyday. Even personal journals, now taking the e-form blogs, have moved into this world wide public forum. With nearly all information and an ever-increasing amount of financial transactions taking place online societies negative elements are sure to follow. Crime goes where the money is and thus the Internet has quickly given birth to a new breed of criminals. Using new methods to accomplish old goals, this new breed of lawbreakers function in a way that has never been seen before, functioning across borders and legal jurisdictions, far outside the realm of traditional law enforcement. The Internet has, to a limited extent, become the new Wild West: lucrative, expanding, and largely lawless.

Many universities have joined the fight by beginning to train a new breed of sheriffs to protect this new e-territory. Like sheriffs of old the line between the criminals and the defenders of justice isn't always as clear as good versus evil. Doc Holliday and Wyatt Earp probably rode the same breed of horses and rode in the same style as Billy Clayton and his band of outlaws. They'd have shot the same sort of firearms, using the same technique, loaded with the same ammunition. Holliday and Earp would have probably been just as able, if not more so, to plan a jailbreak, hijack a stagecoach, or even rob a bank. [1] While this should not be taken as advocating vigilantism in computer security courses it illustrates an intriguing point. In most respects, from

clothing to methods, the law enforcers were little different from the law breakers. Except for a small metal badge carried by the lawmen the only real difference between these very different groups was their motivation. The "how" of doing their job was nearly identical, but the "when", "where", and "why" was completely different. Many of the same "how's" can be used as easily to protect as to attack ([2],[3],[4]).

In very much the same way the digital sheriffs being trained by today's universities, technical schools, and certification programs are learning in the same way. Understanding how to lock down a firewall also shows a student how to cripple one. Teaching a student a tool that enumerates vulnerabilities to be patched also shows them how to enumerate vulnerable machines for exploitation. Although dangerous when misused, these tools are still of great use to an information security professional, when used in the right context. How could law enforcement investigate crimes without understanding how they are committed? How could a police officer keep people safe if he isn't capable of firing his weapon at a dangerous criminal? In the same way that a police officer understands the correct "when", "where", and "why" to fire his weapon, Information Assurance professionals should know the when, and where to use of techniques and tools they possess. This becomes especially relevant when discussing the use of malicious tools.

2. CURRENT CURRICULUM

At Penn State University much work has already been done to provide the best possible learning experience for future Information Assurance Analysts, Engineers, and Managers. Inside the School of Information Science and Technology the Information Assurance program works to educate these future leaders in many aspects of computer security. All Information Assurance students are required to take the standard set of introductory IST courses, including an Introduction to Networking, an Introduction to Databases, and two basic programming courses, one taught in the School of IST and one from the Computer Science department. Once this background is established the Information Assurance specific courses become available. All Information Assurance Track students are required to take the introductory technical course, Network Security, as well as the introductory policy and ethics course, the Legal and Regulatory Environment of Privacy and Security. In addition each student is required to take one additional Information Assurance related course of their choosing, such as Wireless Network Design and Security, Web Application and Database Security, or in some cases an independent study with an Information Assurance track professor.

Laboratory requirements vary from class to class, though typically, as would be expected, the technical courses have a lab component. These laboratory times are conducted outside of class, and are generally dependent on the current lecture track, though this is not always the case. Students in teams of 5 to 8 people work together through a technical lab proctored by a Teacher's Assistant (TA). These labs cover both malicious and defensive tools, giving students a basic overview of their setup and operation. Afterwards students are given a homework sheet with a few basic questions about the technology used and its operation.

The current Information Assurance lab curriculum includes two weeks studying the attack tools Metasploit Framework and L0pht Crack Password Cracker. The other eight weeks of lab detail use of a piece of standard Cisco network defense appliances and technology. Weeks three and four teach the use and maintenance of a Cisco router, weeks five and six are spent learning the Cisco Pix firewall, seven and eight are a Cisco Intrusion Detection System, and the last two weeks round out the series studying a Cisco Virtual Personal Network appliance. All these labs were Cisco approved lab sessions also taught by a graduate student TA.

3. HOLES IN ATTACK UNDERSTANDING

One of the biggest problems in any undergraduate Information Security/Assurance curriculum is balancing the many elements that need to be taught [5]. Computer security is a constantly evolving and changing world, defenders are being pressed to understand and deal with new threats, old threats revisited, and old threats subtly changed. At this point it becomes a struggle to keep up to date and decide what new issues need to be brought to the students attention and what can simply be left for them to discover once they reach their places of employment. On top of this is the difficulty of pacing a course correctly. Computer Security and Information Assurance cover a huge realm, from programming to policy, network administration to system configuration, and now spyware to spam [5]. It's difficult enough for most classes to get through the defensive basics and how to develop security policy. It is often impossible to even begin the most basic overview of attacks such as buffer overflows, configuration exploitation, spyware, spam, and the many other challenges facing individuals, corporations, and governments.

It's quite understandable that defensive technology and the policy of running security in a corporate security is the priority of academic network security courses. The vast majority of Information Assurance students will be working in defensive roles, protecting network infrastructures, not attacking other networks. With the exception of government run and funded Information Warfare, corporate penetration testing, and underground hacking competitions such as Root-Fu or Capture the Flag, very few students will ever put into practice the attacks they're being taught to defend against [6]. This emphasis on defense while largely ignoring the intricacies of attack may be most practical in the short-term view it hurts students in the long run. When Penn State Network Security students were asked the question: "Do you feel an understanding of techniques a malicious hacker would use will benefit you if you go to work in the Information Assurance field?" they unanimously agreed that understanding hacker techniques would further their ability to properly secure information. The same survey also brought to light that a majority of the students actually took personal time after the conclusion of the attack lab sessions to do their own investigation into the tools taught. With this in mind, combined with how little is actually taught about the intricacies of the attacks they eventually will be forced to defend against, students realize that their education omits an important issue of security. In short, defenders can better defend when they have a firm, technical foundation into how the attackers will attack.

4. JUSTIFICATION AND DUE DILIGENCE

With students themselves clamoring for experience in this area the question truly becomes is it necessary? While courses should stimulate students' interest these courses should also be applicable to the students after graduation. In my personal experience I have found skills in evaluating technologies and threats have been far more useful in the business world than my ability to configure appliances. Though defending the network is always the goal, training, firewall configuration, support for setting up VPNs, and instructions for getting an Intrusion Detection System tuned are available. When a company purchases such expensive technologies support for making them work is included. It takes a unique blend of experience, knowledge, contacts, and luck to be able to identify, analyze, and advise on today's threats, this is a combination that is difficult, if not impossible, to teach. [2] Students can however be given a framework from which to continue their learning, and for that it is necessary to teach lab exercises detailing the use of malicious tools. Understanding the configuration of a device is simple, understanding the potential impact of an exploit or tool to an enterprise network is complicated.

Undeniably teaching malicious tools is a double-edged sword. There is a fine line between teaching students to understand a possible attack and giving them the knowledge to carry out such an attack [4]. With every hacker tool that is taught educators risk creating the very menace they are trying to teach students to defend against. This paradox begs the question, how is it that these tools can be taught without simply giving the defenders more to defend against. In order to properly educate students in both the concepts behind a tool and correct ethical use of the tool it takes more than simply demonstrating the tool, but also showing students how it can be used appropriately. [6]

5. PROPOSED SITUATIONAL LAB CURRICULUM

As a proposed solution to this dilemma development was started on a new form of lab exercise to find a way to not simply teach the "how" of using a tool, but also the "when, where, and why". These labs use situations, mostly through involving valid auditing practices where similar tools would be used by corporate or government security teams to test their various defense in an effort to straighten their current position, not to compromise a foreign network [2]. This provides a way to help students understand that a given tool, while inappropriate, and probably illegal, to use without permission, can be a valuable asset when trying to keep malicious attackers at bay. This gives students a perspective to see that a tool is just a tool, and it is the user's implementation of that tool which decides if it is used to improve and protect a given network, or attack and wreak havoc against an unsuspecting target. These situational labs also provide a more real life experience than simply setting up a router and answering a few facts in a corporate style threat analysis report as was the case in former labs.

The beginning of the lab is a fictional situation, or story, into which the rest of the lab takes place [5]. This story details a time when a tool might be used in a valid security improvement context. It may be a password strength audit for a tool like L0pht Crack, or testing the practicality of a newly installed firewall for a tool like NMap, or possibly doing a network vulnerability audit for a tool like Nessus. Students are asked to place themselves in the shoes of an Information Assurance Engineer at a fictional company and use these tools to find out how they can further protect the company. After a brief set of open-ended instructions that encourage exploration and experimentation students are given a set of goals that force the students to properly utilize the tool in the laboratory network environment. These goals fit the context, and help guide the students in solving the problem posed in the context. Students might have to use L0pht Crack to conduct their password strength audit to find what employees are failing to comply with company password policy. They might need to identify unnecessary open ports that the firewall technician failed to lock down by scanning it using NMap, or they could be asked to identify what machines failed to receive the latest Microsoft Update and still have critical holes using Nessus. Each context and problem is tailored to the tool being taught, giving students a perspective on "when, where, and why" to use each tool.

Further reinforcement comes in the changes to the format and goals of the homework given at the end of each lab. Where past labs have had simple questions about typical commands or overarching concepts the new situational labs will continue in the fictional corporate context and require the students to submit their own audit reports. This requirement forces students to think critically as they would when employed by any real world corporation. The L0pht Crack lab would have homework that helps students craft an audit report detailing the amounts of passwords that complied and did not comply with standard company password policy. Furthermore students would create a list of users failing to comply and provide recommendations for remediation of these problems, as well as possible improvements to the policy as it stands. For the NMap lab a detailed report of the firewall box itself, what ports are left open, and any changes that should be made to the firewall policy would be expected. To complete the Nessus lab a

report of patched and unpatched machines would be expected. This gives more of a real world, applicable end to the lab by getting students to complete the audit as would be expected, with a report to management detailing their procedures, findings, and remediation recommendations.

After students progress through five such labs they are faced with a final capstone project before lab curriculum progresses to set of defensive lab with the same emphasis on real world context. Continuing with the idea of context being essential to properly help students understand the use of these tools students are presented with an interesting set of problems in what is by far the most open ended lab. Student teams are put in a situation where they are using the tools they have learned to conduct an open penetration test, given a target of significance on the network and must use the skills they developed using these various tools to take advantage of the vulnerable system. This is not a hack, but an audit, and as a result a similar report to the other tasks is required. Teams are asked to detail the approach they took, the steps and vulnerabilities they used to find their way to the goal, and most importantly, a detailed report of remediation and suggestions for securing this network against their attack methodology, as well as any other possible attack methodologies and approaches.

The use of context and treating the lab like a real exercise are what gives students the "when, where, and why" that is lacking in traditional, procedure based labs. While a step-by-step walk through of a tool might give a student the barest amount of understanding about how to use a tool it is only the application of that tool that makes it valid. Further, in the corporate world, the use of a tool is only as valid as the results it generates, thus it is doubly important that reporting is an integral part of these lab exercises, reinforcing both the labs content, and giving students practice at producing these real world style reports.

6. CHALLENGES AND OPPORTUNITIES

In creating a set of labs that mimics the context of real life security audits, realism is perhaps the most difficult, yet most necessary, characteristic to establish. Students must believe in the possibility of truly being faced with this type of challenge when they enter the working environment for them to fully apply themselves. As labs are continuously created they must constantly evaluate the realism and validity of the situation in which they are used, since simply teaching the tool without a realistic use situation defeats the entire idea of helping students understand the ethical use of these tools. Reporting templates must also follow the labs and uphold the continuity by making the reporting requirements accurate.

Realism in the lab environment, especially for the penetration testing exercise, is essential, making the environment setup incredibly complicated and requiring careful planning. Care must be given to make sure that the objective can be accomplished using whatever group of tools is taught in a given semester. Furthermore, multiple attack methodologies should be valid for accomplishing the given goal. A true to life diversity of clients, servers, appliances, services, and operating systems should be represented. This is complicated by the need to make sure vulnerable versions of operating systems and services are in place in the environment, and that valid attacks and exploits are made available to the auditors, either by pre-configuring their testing host box, or by making the appropriate files available on a resource server or disk.

The detailed reporting provides a challenge over past lab formats as TA's are forced to not simply check objective, short answer questions, but instead to read and evaluate longer, detailed audit reports, where answers may vary greatly, but still be correct. This limits the ability for a professor to simply provide a key to the TA, and instead requires the TA to be extremely familiar and use their own judgment to evaluate the validity of various answers. Lab creators must provide clear guidelines that attempt to remove as much ambiguity as possible from their guidelines of answers and minimize the amount of subjective judgment that those grading the exercises must use.

7. CONCLUSION

Information Assurance educators are faced with a difficult task in the years ahead. With a constantly growing need for Information Assurance professionals and a continuously changing realm of security it is a struggle to maintain both the correct body of knowledge and ethical attitude. Teaching malicious tools provides an essential part of developing a holistic approach and understanding to security. By giving students an understanding of attack methodologies and by allowing them to utilize the same tools malicious attackers use, students develop the holistic understanding of security that they desperately need. By teaching these tools in a context where students can use them ethically they understand not only "how" an attack succeeds, but "when, where, and why" that same tool can be used to keep the bad guys out. Essentially participating in a class that teaches the "when, where, and why" is the sheriff's badge of the new Wild West.

This work was supported by NSF DUE-0416827, and by DoD IA Institutional Capacity Building at Penn State Grant.

REFERENCES

1. "Wyatt Earp." Wikipedia. 2005. 9/21/2005 <http://en.wikipedia.org/wiki/Wyatt_Erp>.
2. Patricia Y. Logan and Allen Clarkson. "Teaching Students to Hack: Curriculum Issues in Information Security." SIGCSE '05 vol 1 2005. p. 157.
3. Laurie Werner. "Teaching Principled and Practical Information Security." Consortium for Computeing Sciences in Colleges vol 1 2004. p. 81.
4. Tom Wulf. "Teaching Ethics in Undergraduate Network Security Courses: The Cautionary Tale of Randal Schwartz." Consortium for Computing Sciences in Colleges vol 1 2003. p. 90.
5. Ed Crowley. "Information System Security Curricula Development." CITC4 vol 1 2003. p. 249.
6. James Harris. "Maintaining Ethical Standards for a Computer Security Curriculum." InfoSecCD Conference vol 1 2004. p. 46.