Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

A Graduate Level Assessment Course: A Model for Safe Vulnerability Assessment

Art Conklin and Gregory White, Ph.D.

Abstract – A graduate level course on security vulnerability assessments, including practical experience at commercial firms, has become a cornerstone of our Information Assurance curriculum. The hands on nature of the course, designing, performing and experiencing an actual team based security assessment significantly deepens the level of understanding for students. Blending academic and training aspects yields a course with significant content and a unique opportunity based delivery mechanism while at the same time providing favorable exposure of the program to the community. The development of the course has been a journey through many challenges most of which are resolved through adequate pre-class preparations. Feedback from students has shown the long term value of a true comprehensive applied course.

Index terms – Security and Protection, Information systems education, Computer and Information Science Education

I. INTRODUCTION

Educating college students to become computer security professionals is a daunting task. The breadth of knowledge required to be an effective computer security specialist is immense. Beyond the theoretical and technical knowledge requirements, additional knowledge is needed in the practical application of a variety of principles. Several different educational methods are used to present students with an opportunity to combine theory and application. One methodology employed at several institutions is the use of a cyber-security exercise. [1-4] Another method is through the use of a vulnerability assessment course including a practical portion involving an actual assessment. We propose that the breadth of knowledge associated with assessments make this a very attractive alternative. In fact, the breadth is sufficient for this course to serve as a capstone option for a computer security curriculum. This paper will outline issues and advantages associated with the use of a vulnerability assessment course in an IA curriculum.

Art Conklin and Greg White are with the Center for Infrastructure Assurance and Security at The University of Texas at San Antonio. Dr. White is in the Computer Science Department and Mr. Conklin is ABD in Information Systems in the College of Business.

A debate has raged for a number of years as to whether it is appropriate to teach individuals how to penetrate systems in order to better prepare them to protect their own systems and networks. Some claim that it is irresponsible to teach individuals skills that could be used in a harmful manner. Often individuals in this camp refer to this type of instruction as "hacker training" implying that what the instructor is doing is creating the next generation of attackers that will create chaos on the Internet. Others feel that in order to understand how to defend a network, administrators need to know how individuals will attack their systems and the best way to do this is to train them on the same tools and techniques that attackers use. This 'attack understanding' point of view is the basis of the US military service academies information assurance programs and cyber-security exercises.[5]

From a technical standpoint, the depth and breadth of material presented in many security classes, results in knowledge that can be used by students to abuse systems. A key difference between the "hacker" course and an assessment course is the focus and approach taken by the instructor. Focusing on understanding and performing vulnerability assessments can be a successful and useful method to help individuals secure their own networks. For the past four years, The University of Texas at San Antonio (UTSA) has presented a course that has provided students an opportunity to learn about network vulnerability assessments and conduct an actual assessment as part of the course. In the course, the students learn the fundamental elements of network vulnerability assessments, including tools and techniques needed to perform these activities. The feedback from all involved - student, faculty, administration and corporate partners - has been very positive. Fears of misuse aside, no adverse reactions or reports of negative activity from students have been observed or received to date.

A comprehensive capstone course is an important part of a graduate level security curriculum. A culminating educational event to combine information previously learned in several classes, coupled with an opportunity to put it all in context, helps complete a level of instruction for the students completing a curriculum. The use of an assessment based course to achieve this aim is significantly different from the use of an exercise based

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

course. Although both can focus on defensive techniques, actual assessments in a real business environment can provide a broader perspective of practical tools and experience. The methodology used in this assessment based course is a blend of training and scholastic approaches.[6] The course depends on prerequisite knowledge of formal methods and models from a scholarly point of view [7,8] which is ensured through previous coursework. The location of the information assurance curriculum within the Information Systems department in the College of Business drives the objective to blend theory with the practical in an operational environment subject to business constraints. This adds to the ultimate utility of the assessment course from a student perspective. Although seemingly simple and obvious to implement, a practical based assessment course has many potential roadblocks. A description of these issues and solutions is presented based on our experience over the past four years.

II. Purpose of the Course

The assessment course is presented as a graduate-level course. Students in the assessment course have previously taken an introductory course in voice and data security and at least one elective course with a security component. The information systems students in the program are different from the average graduate student in the computer science department. Most are non-traditional students who are returning to school while holding jobs in industry or with the government. They are mostly U.S. citizens and on the average are a few years older than the average computer science graduate student and typically have several years of work experience in the computer industry. The age and work experience factors play a role in the level of expected performance.

The design of the assessment course is centered around three foundational elements; theory, people and practicum. The first foundational element is to provide the students a theoretical understanding of the reasons why network systems are vulnerable to attack. This involves more than an enumeration and simple discussion of the reasons that specific technical vulnerabilities exist. It involves an examination of why security in an operational environment is difficult to obtain for most organizations. The second foundational element is the role of people in the computer security equation. Understanding the human aspect of security is a critical aspect of understanding why organizations have so much difficulty in securing their systems and networks. The third element, practicum, involves the students in an actual assessment in the field on an operational system. This involvement is from the beginning planning stage, through the conduct of the assessment, to the finished report and presentation. This experience adds to the foundational elements by introducing issues such as ethical conduct, professionalism, and an opportunity to witness actual organizational concerns over sensitive data.

The course serves several functions in the education of the graduate student. There is a marriage of theory and practical exercise that is demonstrated in a real-world commercial environment. This exposes students to where security theory meets business reality and allows them first-hand to experience issues associated with actual security management. The course also acts as an integrator of theories, practical tasks and business, providing an opportunity for students to put it all together, combining people issues, technical issues and business reality.

III. Structure of the Course

The course is roughly divided into three segments. The first covers the organizational and procedural aspects of performing and reporting the results of a vulnerability assessment. Also included in this are the policies, procedures, and training that an organization should maintain as part of an effective security program. The second segment covers the technology required to perform an assessment and examines vulnerabilities from a technical perspective. This segment is where the majority of the lab work takes place as students have an opportunity to explore the technical aspects of performing a test in the safe environment of the laboratory. In the last segment of the class the majority of the actual assessment work will be conducted. While preliminary meetings were held early in the semester, and specific documents developed outlining the tests to be performed as agreed upon by both parties, the actual tests are designed to be conducted after the students have had an opportunity to practice on a sample organizational network in a controlled environment.

To assess student performance in the class, a multiple assessment method is used. An exam can cover the material presented in the first part of the course. A final exam can also be used to assess overall learning of both principles and how they are applied during the assessment. Grading of the deliverable report is done on a contributor level, with the instructor assessing each contribution as the edit cycle of the report is performed. For oversight and safety, the instructor is an integral watchdog of communications between the students and the firms being assessed, with all materials undergoing pre-release review. Although this adds significantly to

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

the time commitment for the instructor, this review provides a good grading opportunity.

A. Preparatory Segment

In the first segment, the preparatory phase, students learn about the organizational and procedural aspects of conducting a vulnerability assessment. These tasks are primarily taught in a lecture mode, with homework and group exercises supporting the lectures. As the final project of the class is an actual assessment, any preparatory work for that assessment, including non-disclosure agreements, communication plans and schedules are also addressed in this portion of the course. This segment, although the shortest of the three, provides a foundation for the rest of the course. The plans, schedules and documentation from this segment will be used in later segments to guide the actual assessment. Since a major portion of the class are the actual assessments the students will perform, a key part of preparatory instruction involves an understanding of the methodology used to conduct the assessment. A five-phase approach is used patterned after the methodology found in one of the two texts used in the course. The five phases are data collection, evaluation, analysis, draft report preparation, and final report presentation. [9] For the course, the data collection and evaluation phases are roughly broken into three parts: an external assessment, an internal assessment, and an examination of the organization's policies, procedures, and training.

B. Practical Tool Segment

The second segment of the course is an active hands-on learning phase designed to acquaint the student with the tools used in an assessment. Although an assessment is comprised of more than just a technical examination of network security, the technical examination forms a large component of the assessment. This is the portion of the course most open to criticism, yet learning how to use vulnerability assessment tools is an essential part of a complete security education. Whether looking up a vulnerability in a database, learning to use a network scanning tool, or learning to sniff wireless packets, the focus must remain on the role these items play in an assessment and in securing a network. Consistent and frequent discussions of the powers and dangers of these tools are important, as is the use of open discourse concerning the importance of ethical behavior in the computer security profession.

Since it is important that all students understand each phase of the assessment, labs supplement the assessment to provide the students with additional experience, for which they also receive feedback in the form of comments and a grade. An assessment laboratory has been created which includes a target network, not accessible to the outside world, with various operating systems, applications, and vulnerabilities. The students have the opportunity to test tools before they are used on an operational network owned by the client and can become familiar with the various options each tool offers. Focusing each laboratory assignment on using the tools in a proper context, i.e. as part of an assessment, rather than just spending time exercising tools provides incentives for the students to learn the tools.

C. Assessment Segment

The third segment of the course entails the actual assessment, in which one or more actual assessments are performed on local organizations. The number of assessments is determined by several factors, class size, number of available firms and lastly, instructor time and experience. As the instructor is a key player on all assessment teams, as an observer and safety mechanism, if too many assessments are attempted, instructor time may become a big issue for client meetings and event coordination. Over the past four years, we have progressed from a single to three concurrent assessments with a class size of 25 students.

The assessments consist of three parts, portions of which can be conducted concurrently. In the external assessment, students take the role of a technically savvy but uninformed external attacker. They conduct an assessment of the organization's public presence, learning what they can about it. They attempt to determine URL's, IP addresses, phone numbers, employee names, and other pieces of information often not considered sensitive in nature. Before actual penetrations or even scans are attempted the information obtained is verified with the organization's point of contact. Doing so ensures that correct IP addresses and phone numbers are tested when the technical portion commences. Once the information is verified, the students can begin scanning and penetration activities. All such activity has been carefully discussed with the organization and specific tests agreed upon by all parties, including the instructor, in advance. Tests are also conducted from a specific IP address so that the organization can determine if a detected attack is part of a test initiated by the students or is an actual attack from another individual. An emergency contact number is supplied to the organization so that in the event that a test causes an unexpected disruption of service the

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

organization can call for the immediate termination of the test. The goal of this phase is to determine what vulnerabilities may exist in the network and whether unauthorized access can be obtained or sensitive information collected. All log files and records are kept from these tests, even if unsuccessful, to be provided to the organization with the final report.

The second part, the internal test, is conducted from the perspective of a normal employee of the organization. Supplied with a normal user-level account, students pursue a goal to attempt to elevate their level of permission on the system and to obtain access to sensitive information that the employee should not have access to. The students bring tools with them on CD or floppy and will attempt to load and run them on the system to which they are given access. Like the previous phase, this phase includes a physical security check as well. The students will attempt to locate passwords in common hiding places (on calendars, under photos, in drawers) under the supervision of the organization's representative and will also attempt to connect their own equipment to network drops they have access to.

The third part of the assessment, which may be conducted concurrently with the other two, is an evaluation of the organization's policies, procedures, and training. The organization's point of contact is asked to supply current policies and procedures and these are compared against similar best practices in the same industry. Allowances must admittedly be made for different environments but industry best practices provide a place to begin the analysis from. The training program and materials will also be evaluated and a questionnaire developed and offered to the organization to conduct a survey to determine the effectiveness of current training practices. As part of this team's responsibilities, log files from systems are analyzed to determine if possibilities to improve on current mechanisms exists. This also provides an opportunity to evaluate security and operational baselines or to encourage the establishment of them in order to better be able to determine the current security posture of the organization.

After all the data collection has occurred from the three different parts of the assessment, each group independently meets and drafts their sections of the report. As the report is being built, the team leaders meet and decide upon the main points to emphasize in the report and the primary findings. After all three sections are drafted; the team leaders take the report as a whole and resolve formatting and writing style issues. A briefing is prepared along with slides, a formal report and an executive summary. These are all reviewed by the instructor prior to the final meeting with the assessment client. This final meeting can take many forms, sometimes only a couple people representing IT for the client are present, at other times it is a significant show with managers and users attending. In all cases, the focus is on delivering a professional presentation of clearly prioritized issues and findings. It should be noted that once the final report is delivered and accepted any remaining working papers are destroyed. This is one of the items spelled out in the agreement between the entities.

IV. Issues That Must Be Addressed

While it may seem that conducting this course is fairly straight forward and mimics the actions that a security consultant might take in performing a security test on an organization, it is not that simple. The actual tests conducted as described are similar as well as much of the documentation that accompanies an assessment. A large difference, however, are all the safeguards introduced at each phase to protect all parties. Although these safeguards add significantly to the coordination and communication tasks and impact the speed of the assessment, these very safeguards form the basis for trust. Developing a level of trust and comfort between all parties is essential. The university administration has to be convinced that this activity is beneficial to the students and program and any risks are minor, understood and worth taking. It is imperative that instructors contemplating conducting a course such as this inform the appropriate administration officials of their intention and the possible problems with the course. Early explanation of the risks and the plans to manage the risks is essential in gaining the trust and confidence of the university administration. There are several important documents that must be included as part of the preliminary meetings with potential organizations.

An essential document is the statement of work that is drawn up and agreed upon by both the class and the organization being assessed. In this document the scope of the tests is clearly identified. Whether social engineering or denial of service tests may be conducted is explicitly spelled out. The dangers of conducting a test are identified and explained along with the possible ramifications. The document also clearly identifies the safeguards the class will invoke to minimize the likelihood that a problem will occur. This document will also grant the specific permissions necessary to permit the lawful assessment of the company's network by the students.

Another important document, especially from the point of view of the organization that is having the assessment done on them, is a non-disclosure agreement that all students are required to sign. In this document the

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

students agree to not divulge any proprietary information that they come in contact with should any of their tests be successful. They also agree not to divulge the results of any of their tests and in fact agree not to identify the organization that they conducted the test on. A student not wishing to sign such a document is not allowed to participate in the assessment and alternate assignments must be provided for the student to accomplish. Most universities, especially those conducting research, will probably already have a standard nondisclosure agreement that can be used for the purposes of this class. If one does not exist, it will have to be created and approved by the academic institution's legal counsel before being used.

One factor to consider when choosing a partner for the assessments is to choose a firm where the students would have nothing to personally gain from the specific knowledge learned. This is the primary reason that the assessment is not performed on the university itself, for the information gained and future access are a combination best avoided. In fact, all laboratory work can be conducted from an isolated laboratory, with no connection to the rest of the university network to ensure this separation. Additionally, when outside Internet access is used for the penetration testing, it is done from a specially controlled setting from the isolated lab, so that errors can be immediately corrected and activity monitored.

A key element in making everything work is communication between all parties, the instructor, the students, the firm and the university. Because of the sensitive nature of the actions involved in an assessment, clear communications must be maintained between the client organization and the assessment team. This is the primary role of the project leader and each team leader. All actions are discussed and "approved" before implementation, with approval required by both the course instructor and the organization being assessed. Having a clear open communication channel, with regular meetings and positive feedback of true communication is essential in the safe performance of the individual tests. The final form of open communication is in the outbrief, where the project leader briefs the client organization on their findings and turns over all logs and working materials.

V. Benefits of the Course

There are a number of benefits in providing a course on conducting a vulnerability assessment. While some may argue that it is not necessary to learn how to attack a system in order to learn how to defend it, there are many others who would disagree and argue that it is very beneficial. [5] Knowing what tools exist and how they are used to attack systems seems to be valuable in understanding how to defend against attacks by these tools. There is also a certain benefit in "taking the other side" to obtain a different view of the problem. Frequently this will reveal vulnerabilities that might not have been noticed when looking at the issue from a defensive standpoint alone. There is also a certain appeal in attacking systems that adds to the excitement of learning for the students and keeps them engaged in the course. Another benefit for the students is realized in the project management portion of the assessment. Several of the students will obtain experience in organizing and managing a team of individuals who must work together on the project. While this is not one of the stated goals of the course, it is certainly one of the byproducts of it for several students.

Providing an assessment for organizations in the community that would not be able to afford them otherwise helps to foster better community relations for the university. This is especially true for non-profit organizations who generally don't have the financial means to hire a consultant to conduct an assessment and who also frequently conduct fund raising projects that might include maintaining records of credit card information. Since these organizations are often staffed by volunteers, the likelihood that the organization spends any appreciable amount of time on security is low. One factor that lessens the community finding out about the university's efforts on the behalf of the assessed organizations is of course the fact that the instructor and students have agreed not to reveal who they conducted the assessment on. Just as in industry where referrals are important but often sometimes hard to obtain for security companies, referrals may be hard for the university to obtain. Since only a limited number of these can be conducted, however, this issue is not as critical for the academic institution. A key to managing this aspect is building a solid reputation as trustworthy and helpful, as this aids immeasurably when approaching potential industry partners.

How effective the course has been is clear; after four offerings in the last four years – over 100 students have taken the course and have performed 8 assessments. One firm has been involved for three years, highlighting the power of relationships, even when this firm's management has changed each year. The true success measure has come from the former students, who have provided very positive feedback on the usefulness of the course and how it has helped them in their current jobs. These results are all due in great part to the carefully crafted curriculum detailed above that has produced a course that serves as a capstone in a graduate security curriculum. In the final analysis, we believe that courses such as the one described above add significantly to a

ISBN 1-933510-99-4/05/$15.00

security program and provide experience that is impossible to duplicate in a laboratory environment. If very carefully managed, the risks of teaching such a course are far outweighed by the benefits to the students of the course.

VI. References

1. Lance J. Hoffman and Daniel Ragsdale, Exploring a National Cyber Security Exercise for Colleges and Universities, Report No. CSPRI-2004-08 The George Washington University Cyber Security and Policy Research Institute Report No. ITOC-TR-04001 United States Military Academy Information Technology and Operations Center August 24, 2004
2. W. J. Schepens, D. J. Ragsdale, and J. R. Surdu, The Cyber Defense Exercise: An Evaluation of the Effectiveness of Information Assurance Education, The Journal of Information Security, Volume 1, Number 2. July, 2002.
3. G. Vigna, Teaching Hands-On Network Security: Testbeds and Live Exercises, Journal of Information Warfare, vol. 3, no. 2, pp. 8-25, 2003.
4. D.W. Welch, D.J. Ragsdale, and W.J. Schepens, Training for Information Assurance, IEEE Computer, March 2002.
5. Don Ragsdale, Don Welch, and Ron Dodge, Information Assurance the West Point Way, IEEE Security and Privacy, vol. 1, no. 5, Sept/Oct 2003, pp. 64-67
6. Matt Bishop, Computer security education: training, scholarship, and research, IEEE Computer, April 2002.
7. C.E. Irvine and T. Levin, Teaching Security Engineering Principles, Proceedings of the World Conference on Information Security Education, Perth, Australia, 12 July 2001.
8. Cynthia E. Irvine, Teaching Constructive Security, IEEE Security and Privacy, vol. 1, no. 6, Nov/Dec 2003, pp. 59-61.
9. Thomas R Peltier, Justin Peltier, and John Blackley, Managing a Network Vulnerability Assessment, Auerbach Publications, Boca Raton, 2003.

ISBN 1-933510-99-4/05/$15.00