6-2017

The Development of an Applied Ethical Hacking and Security Assessment Course

Jacob Young
Bradley University, jayoung@fsmail.bradley.edu

Kerstyn Campbell
Bradley University, kncampbell@mail.bradley.edu

Angelica Fanti
Bradley University, afanti@mail.bradley.edu

Samantha Johnson
Bradley University, smjohnson2@mail.bradley.edu

Zachary Sells
Bradley University, zsells@mail.bradley.edu

See next page for additional authors

Recommended Citation

Young, Jacob; Campbell, Kerstyn; Fanti, Angelica; Johnson, Samantha; Sells, Zachary; and Sutter, Alex, "The Development of an Applied Ethical Hacking and Security Assessment Course" (2017). *MWAIS 2017 Proceedings*. 40.
http://aisel.aisnet.org/mwais2017/40

Authors
Jacob Young, Kerstyn Campbell, Angelica Fanti, Samantha Johnson, Zachary Sells, and Alex Sutter

The Development of an Applied Ethical Hacking and Security Assessment Course

Jacob A. Young
Bradley University
jayoung@fsmail.bradley.edu

Kerstyn N. Campbell
Bradley University
kncampbell@mail.bradley.edu

Angelica N. Fanti
Bradley University
afanti@mail.bradley.edu

Samantha M. Johnson
Bradley University
smjohnson2@mail.bradley.edu

Zachary S. Sells
Bradley University
zsells@mail.bradley.edu

Alex M. Sutter
Bradley University
asutter@mail.bradley.edu

ABSTRACT

Information security education in higher education has made substantial progress. However, despite advancements in pedagogy and the technology used in the classroom, students often yearn for more applied opportunities. Further, small businesses are likely to have inadequate information security postures due to limited budgets and expertise. In order to address both issues, we have developed and are currently piloting an advanced course in ethical hacking which allows students to perform security assessments for local businesses. This paper will assist academics in the implementation of similar courses, which not only improves security education for students, but can also increase opportunities for local businesses to receive affordable security assessments.

Keywords

Security, security assessment, penetration testing, social engineering, security education, pedagogy

INTRODUCTION

Information security education in higher education has made substantial progress. However, despite advancements in pedagogy and the technology used in the classroom, students often yearn for more applied opportunities. Further, small businesses are likely to have inadequate information security postures due to limited budgets and expertise. In order to address both issues, we have developed and piloted an advanced course in ethical hacking which allows students to perform security assessments for local businesses. The goal of the course is to provide students with an opportunity to plan and perform a security assessment for a live-client. In doing so, students gain technical experience by utilizing offensive techniques while simultaneously developing the adversarial mindset necessary for defense. In this paper, we outline the structure of the class and necessary requirements, as well as provide insight into some of the successes and challenges we faced throughout the semester. This paper will assist academics in the implementation of similar courses, which not only improves security education for students, but can also increase opportunities for local businesses to receive affordable security assessments.

COURSE DEVELOPMENT

This course employs a service-learning (Furco, 1996) approach to security education. As shown in Figure 1, Service-learning equally balances academic objectives with the service being provided to the client. This requires the service project to be fully integrated into the course. Doing so allows the students to provide a valuable service in the process of learning how to perform security assessments. Aside from client recruitment, which is conducted by faculty and staff, the students are involved in every step of the security assessment. This results in a classroom environment where each student is expected to immerse themselves into the project in order to identify opportunities for exploration on behalf of the client. Instead of providing direction, the instructor simply facilitates the course by supervising and offering guidance to the students. The structure of the security assessment process closely follows the National Security Agency's INFOSEC Evaluation Methodology (IEM) (Rogers, Fuller, Miles, & Cunningham, 2005) and INFOSEC Assessment Methodology (IAM) (Rogers, Miles, Fuller, Hoagberg, & Dykstra, 2004). However, due to the wide variety of tasks that students might want to pursue, the instructor will often need to point students to specific resources for particular activities.

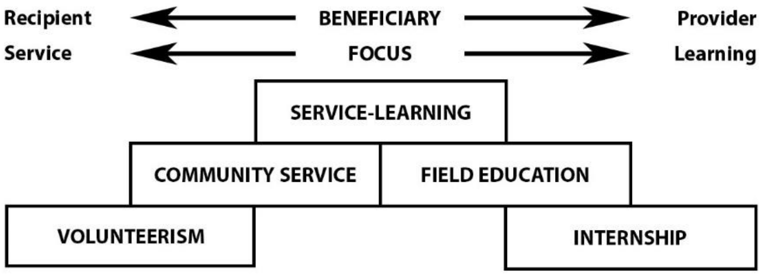

Figure 1. Distinctions Among Service Programs (Furco, 1996)

Client Recruitment

Client recruitment was strengthened by the strong reputation developed over the course of decades of institutional experience with managing student consulting projects. Due to the risks associated with performing live security assessments, client recruitment for this course was initially limited to organizations with established student-consulting relationships. Future client recruitment will eventually extend to new organizations once the course has been refined and proven success can be better demonstrated.

Industry Partners

Throughout the development process, we engaged with a number of professionals in order to gather feedback and guidance. These industry partners provided assistance with the operational logistics, legal challenges, and security assessment expertise. Those who wish to offer a similar course at their institution are encouraged to seek assistance from industry partners such as information security firms, Internet service providers (ISPs), law enforcement agencies, and attorneys.

Legal Considerations

Due to the sensitive nature of such work, it is absolutely imperative that all legal issues are properly considered. Businesses interested in commissioning security assessments are encouraged to obtain legal counsel. This ensures that the work-product would be protected by attorney/client privilege. This step is critical for a couple of important reasons. Should the client ever be the subject of a lawsuit due to a data breach, not only is the client protected from divulging the vulnerabilities uncovered by the assessment, but it also protects the assessment team (faculty and students) from being forced to testify about their involvement.

After discussing the project with the client, a letter of agreement was carefully crafted, which outlined the scope and limitations of the proposed assessment. A signed letter of authorization that contained contact information for the client and specifically outlined the names of the individuals involved in performing the security assessment was also obtained. This provides the assessment team with the colloquially named “get out of jail free card.” However, relying solely upon this document is not sufficient, especially if the assessment will consist of any activities conducted on the client’s premises. In these cases, we strongly encourage faculty members managing these assessments to inform local law enforcement agencies, including the local office of the Federal Bureau of Investigation (FBI), that proper authorization has been obtained prior to initiating any assessment activities.

Prior to the client being revealed to the students, they were required to sign both a white hat agreement and non-disclosure agreement. Further, in order to reduce the likelihood of accidental disclosures outside of class meetings, students are prohibited from referring to the client organization by name. Instead, all references must simply refer to “the client” in order to form a habit that will carry on outside of the walls of the classroom. Students were also strictly forbidden from executing any task without proper authorization from the faculty member. Proposed assessment tasks were submitted for consideration during the planning phase, which allowed for further refinement by the faculty member and other students. Once the assessment team had satisfied all concerns associated with the particular task, the faculty member would authorize the task to be scheduled.

Equipment, Tools, and Resources

The course activities require specialized equipment, tools, and resources in order to perform the security assessment in an organized and efficient manner. A separate server was implemented to host multiple Kali Linux (https://kali.org) virtual machines (VMs), which also provided students with remote access to Maltego (https://www.paterva.com/web7), Armitage (http://fastandeasyhacking.com), and Phishing Frenzy (https://phishingfrenzy.com).

Students were provided access to multiple additional resources to assist them in performing specialized tasks as needed. All students followed the NSA IEM (Rogers et al., 2005) and IAM (Rogers et al., 2004). Students involved in performing reconnaissance and open source information gathering followed the guidance of Bazzell (2016). Social engineering methodology was primarily obtained from Hadnagy (2011) and Talamantes (2014). Advanced instruction for performing specific tasks using Kali was obtained from Weidman (2014), Kim (2015) and Dieterle (2016).

COURSE IMPLEMENTATION

The three-hour course described in this paper was taught over one 15-week semester. Due to scheduling limitations, this course consisted of one scheduled weekly meeting of three hours. Future offerings will be scheduled for two weekly meetings of one hour and fifteen minutes each.

Prerequisite Knowledge and Abilities

For the first offering of this course, the instructor invited eleven high performing undergraduates majoring in management information systems (8), computer information systems (2), and computer science (1) to enroll and participate. The course roster included two juniors and nine seniors comprised of seven males and four females. Each student was either concurrently enrolled in or had already completed the requisite coursework in networking and information security. The mix of various majors provided a diverse pool of skills that allowed students to apply their talents to specialized tasks best-suited to their background and interests. In addition to encouraging more females to pursue careers in technology, the high level of female involvement has a number of benefits for this particular course. For example, due to the stereotypical image of black-hat hackers being primarily male, we feel that the involvement of female students significantly contributed to the success of the social engineering tasks performed as our targets were less likely to suspect an attack from females.

Assessment Phases

This course is conducted in three phases throughout the semester: Information Gathering, Task Execution, and Report Generation. A number of tasks are identified and assigned to various project teams responsible for assessing physical security, network security, social engineering vulnerabilities, and organizational policies.

Information Gathering

One month was allocated to the Information Gathering phase and involved all students participating in the collection of public information about the client organization. Small teams scoured the Internet for various types of information, such as social media accounts (e.g., Facebook, LinkedIn, Twitter) of employees, job postings, customer lists, and physical location details. All of the information was stored into a centralized repository in order to increase team awareness. Based upon the information gathered, tailored assessment tasks were developed for the execution phase.

Task Execution

A number of network scans were performed to assess the security posture of the client's systems. A number of vulnerabilities were identified and targeted for exploitation. This phase also consists of various social engineering attacks, such as vishing and phishing, as well as physical security assessment via site visits and dumpster diving (Hadnagy, 2011). It is important to note this particular client did not limit the types of assessment activities that we were allowed to conduct against their organization. However, it is likely that future clients will not be as willing. Therefore, the tasks performed during our assessment might not be possible for subsequent assessments conducted as part of this course.

Report Generation

The final phase consists of condensing the hundreds of pages of information and results into an easily digestible report for the client. In lieu of a final exam, the students will present their findings to the executive team of the client organization during their regularly scheduled final exam period.

PROJECT MANAGEMENT

In order to ensure that assessment tasks and other class activities are completed on schedule, all students must submit a weekly activity report. In addition, each small group responsible for the planning, execution, and reporting of each of the assigned tasks is required to present their progress to the class on a regular basis. It is also important to note that many of the assessment tasks must be performed outside of the scheduled meeting times for the course. Therefore, the faculty member must be willing and available to supervise these activities.

CHALLENGES FACED

The course was offered a year earlier than planned in order to make it available to the group of students recruited to participate in the pilot. A large majority of these students were on schedule to graduate within the next three semesters. While we were fortunate to successfully implement this course in a condensed timeframe, we highly recommend ensuring that adequate time is allotted to develop the necessary infrastructure and complete all of the pre-assessment steps.

COURSE OUTCOMES

This course generated a number of beneficial outcomes. First, the students benefited by gaining practical experience by conducting a real-life security assessment. Opportunities to participate in the academic research process, including authoring research papers and presenting at conferences, were also made available. Second, the client benefited from the performance of a low-cost, but effective security assessment. By publishing a client-approved version of our findings, the assessment will also assist in improving the security practices of other organizations. Third, the course instructor benefited by discovering new research opportunities in security. Lastly, the institution benefited from the positive public response and increased external engagement, which can result in the generation of additional consulting opportunities.

FUTURE DEVELOPMENT

Due to the success of the course, it will now be offered on an annual basis and included in a newly developed concentration in cybersecurity within the management information systems major. A seat increase will potentially allow for up to three clients to be assessed simultaneously. Experiences from this course will be introduced to students earlier. For example, additional training on social engineering methods, as well as the assessment tools employed, such as Kali Linux and Phishing Frenzy, can be provided in a virtualized lab environment during the prerequisite information security courses in anticipation of the students' matriculation to the advanced course, which will reduce the learning curve.

CONCLUSION

While the course requires careful planning and oversight, the course outlined in this paper has provided students with valuable, real-life experience that is already being well-received by prospective employers. The further development and evolution of this course will only strengthen the course offerings at our institution and further enhance the security of the client organizations willing to participate.

ACKNOWLEDGEMENTS

First, we would like to thank our client, who shall forever remain nameless, for allowing our students to have this opportunity. This course would not have been possible without their faith in our ability to perform a thorough and professional assessment of their security posture. Second, we would like to thank many individuals at Bradley University for their support of this effort, but especially my colleagues Dr. Matt McGowan and Dr. Paul Stephens, as well as Mr. Jim Foley, director of the Turner Center for Entrepreneurship. Thank you for believing in our vision for this course. Lastly, we would also like to thank the reviewers for their insightful feedback. Your suggestions are much appreciated.

REFERENCES

Bazzell, M. (2016) Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information (5th ed.), CreateSpace Independent Publishing Platform, North Charleston, South Carolina.

Dieterle, D. W. (2016) Basic Security Testing with Kali Linux 2, CreateSpace Independent Publishing Platform, North Charleston, South Carolina.

Furco, A. (1996) Service-learning: A Balanced Approach to Experiential Education *Expanding Boundaries: Serving and Learning*, Corporation for National Service, Washington, D.C.

Hadnagy, C. (2011) Social Engineering: The Art of Human Hacking, Wiley, Indianapolis, Indiana, Indiana.

Kim, P. (2015) The Hacker Playbook 2: Practical Guide to Penetration Testing, CreateSpace Independent Publishing Platform, North Charleston, South Carolina.

Rogers, R., Fuller, E., Miles, G. & Cunningham, B. (2005) Network Security Evaluation Using the NSA IEM, Syngress, Rockland, MA.

Rogers, R., Miles, G., Fuller, E., Hoagberg, M. P. & Dykstra, T. (2004) Security Assessment: Case Studies for Implementing the NSA IAM (1st ed.), Syngress, Rockland, MA.

Talamantes, J. (2014) The Social Engineer's Playbook: A Practical Guide to Pretexting, Hexcode Publishing, Woodbury, MN.

Weidman, G. (2014) Penetration Testing, No Starch Press, San Francisco, CA.