Ethical Hacking in Information Security Curricula

Zouheir Trabelsi, College of Information Technology, United Arab Emirates University, Al Ain, United Arab Emirates
Margaret McCoey, La Salle University, Philadelphia, PA, USA

ABSTRACT

Teaching offensive security (ethical hacking) is becoming a necessary component of information security curricula with a goal of developing better security professionals. The offensive security components extend curricula beyond system defense strategies. This paper identifies and discusses the learning outcomes achieved as a result of hands-on lab exercises which focus on attacking systems. The paper includes the ethical implications associated with including such labs. The discussion is informed by analyses of log data on student malicious activities, and student survey results. The examination of student behavior after acquiring these skills demonstrates that there is potentially a high risk of inappropriate and illegal behavior associated with this type learning. While acknowledging these risks and problems, the paper recommends that curricula should opt for a teaching approach that offers students both offensive and defensive hands-on lab exercises in conjunction with lecture material. The authors propose steps to minimize the risk of inappropriate behavior and reduce institutional liability.

KEYWORDS

Ethical Hacking, Ethical Implications, Information Security Curriculum, Offensive Security Techniques

1. INTRODUCTION

The importance of experimental learning has long been recognized in the learning theory literature (Denning, 2003; Du, Jayaraman, & Gaubatz, 2010). Despite this fact many graduate and undergraduate courses in information security still offer a limited number of hands-on laboratory exercises. The need for using a theory and practice-oriented approach in information security education is seen as paramount (Chiou Chen & Lin, 2007). A program that covers only the theoretical aspects of information security may not prepare students for overcoming the difficulties associated with the efficient protection of complex computer systems and information assets. Furthermore a learning environment that does not give the student an opportunity to experiment and practice with security technologies does not equip him/her with the skills and knowledge required for doing research and development in the computer security field.

So far most information security courses have supplemented content by adding a practice-oriented component which includes laboratory exercises (labs) based on defensive information security techniques (Hill, Carver, Humphries, & Pooch, 2001; Mullins et al., 2002; Vigna, 2003; Whitman, Mattord, & Green, 2014; Trabelsi, Hayawi, Al Braiki, & Mathew, 2013). However many academics and industry practitioners feel that to defend a system one needs a good knowledge of the attacks a system may face (Arce & McGraw, 2004). Students who understand how attacks are designed and launched will be better prepared for opportunities as security administrators rather than those without such skills (Logan and Clarkson, 2005). As a result, interest for including labs...
on offensive techniques originally developed by hackers has grown significantly. Teaching ethical hacking techniques has become a vital component of programs that aim to produce competent information security professionals (Brutus & Locasto, 2010; Damon, Dale, Land & Weiss, 2012; Dornseif, Gärtner, Holz & Mink, 2005; Ledin, 2011; Mink & Freiling, 2006; Trabelsi & Al Ketbi, 2013; Trabelsi, 2011; Yuan & Zhong, 2008; Trabelsi et al., 2013).

Adding hacking activities to the information security curriculum raises some variety of ethical and legal issues. By using log data as well as data gathered through a student survey, this paper investigates the ethical implications of offering hands-on lab exercises on attack techniques in information security education. The paper emphasizes teaching offensive techniques which are central to better understanding the hacker’s thinking and the ways in which security systems fail in these situations. Moreover, hands-on labs using attack techniques allow students to experiment with common attack techniques and consequently allow them to implement the appropriate security solutions and more efficiently protect the confidentiality, integrity, and availability of computer systems, networks, resources, and data. The paper proposes measures that schools and educators can take to develop successful and problem-free information security programs while reducing legal liabilities, preventing student misconduct, and teaching students responsible behavior.

The paper is organized as follows: Section 2 presents the case of teaching offensive techniques in hands-on lab exercises and the expected learning outcomes resulting from this approach. Sections 3 and 4 discuss the risks arising from teaching offensive techniques in an academic environment, the associated ethical concerns, and the emerging liability issues; along with practical steps to mitigate these risks. Finally, Section 5 summarizes the results and concludes the paper.

2. TEACHING OFFENSIVE TECHNIQUES: APPROACHES AND OUTCOMES

The overall purpose of applying a hands-on approach to teaching information security is to provide students with demonstration of theoretical concepts through controlled practical exercises using offensive and defensive strategies. The laboratory exercises developed for this type of course need to be relevant to the course curriculum and need to be compatible with the existing laboratory environment so that the setup is affordable. Furthermore the exercises need to be sufficiently simple in order to fit in with the time allocated for the lab, and portable so that they can be easily implemented in different operating system environments and hardware and software platforms.

From each laboratory exercise students learn how to perform a specific attack, and how to prevent malicious hosts from performing it successfully. The learning objective is included in the laboratory exercise manual which also contains descriptions of the attack and the corresponding security solutions. While students would have already covered the information security aspects of each attack in the lecture class, the laboratory exercise begins with summarizing the theoretical concepts related to the attack under consideration. Next students are asked to perform the exercise tasks within the lab time frame. They are given instructions about how to set up and configure an isolated laboratory network, how to generate the attack, and how to implement and test appropriate defensive solutions. Normally students work in small groups of three to four members. Each group’s isolated network may include one victim host and two or three malicious hosts used to generate the attack traffic.

Several outcomes are expected to be achieved as a result of using the teaching and learning approach described above. First students will be able to develop some of the “soft” skills required for information security graduates, including communication and persuasion skills especially when using social engineering techniques. Leadership and team work will be also developed since students work in teams and gain a chance to act as team leaders and team members. Students will also acquire a sense of accomplishment when they successfully break into a system, and a sense of pride when they successfully defend a system. They learn a valuable lesson in persistence and the ability to work within a time constraint on a specific set of objectives.
Pedagogical Teaching and Learning
www.igi-global.com/chapter/pedagogical-teaching-learning/55155?camid=4v1a

An Adaptive Course Generation Framework
www.igi-global.com/chapter/adaptive-course-generation-framework/61964?camid=4v1a