Chapter 11
Teaching Offensive Lab Skills:
How to Make It Worth the Risk?

Zouheir Trabelsi
UAE University, UAE

Margaret McCoey
La Salle University, USA

Yang Wang
La Salle University, USA

ABSTRACT

This chapter identifies and discusses the learning outcomes to be achieved because of hands-on lab exercises using ethical hacking. It discusses the ethical implications associated with including such labs in the information security curriculum. The discussion is informed by analyses of log data on student malicious activities, and the results of student surveys. The examination of student behavior after acquiring hands-on offensive skills shows that there is potentially a high risk of using these skills in an inappropriate and illegal manner. While acknowledging the risk and the ethical problems associated with teaching ethical hacking, it strongly recommends that information security curricula should opt for a teaching approach that offers students both offensive hands-on lab exercises coupled with ethical practices related to the techniques. The authors propose steps to offer a comprehensive information security program while at the same time minimizing the risk of inappropriate student behavior and reducing institutional liability in that respect and increasing the ethical views and practices related to ethical hacking.

INTRODUCTION

The importance of experimental learning has long been recognized in the learning theory literature (Denning, 2003). Despite the fact many graduate and undergraduate courses in information security still offer a limited number of hands-on laboratory exercises as part of the curriculum the need to use a theory and practice-oriented approach in information security education is seen as paramount (Chiou & Li Lin, 2007). A program that covers only the theoretical aspects of information security may not

DOI: 10.4018/978-1-7998-0238-9.ch011

prepare students well 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 students an opportunity to experiment and practice with security technologies does not equip them with the skills and knowledge required for doing research and development in the computer security field. The introduction of information security courses aimed at offering a practice-oriented component have been well received by students (Hartley, 2015). However, review of literature acknowledges the issues of the ethical dilemma associated with these components (Hartley, 2015; Pike, 2013; Wang, McCoey, & Zou, 2018). Some programs enhance their offerings by adding a practice-oriented component that includes laboratory exercises (labs) based on defensive information security techniques (Hill, Carver, Jr., Humphries, & Pooch, 2001; Special Report on Forensic Examination of Digital Evidence, 2004; Vigna, 2003). 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 than those without such skills (Logan & Clarkson, 2005). As a result, interest in incorporating labs on offensive techniques originally developed by hackers has grown significantly (Brutus, Shubina & Locasto, 2010; Damon, Dale, Land & Weiss, 2012; Ledin, 2011; Trabelsi & Al Ketbi, 2013; Trabelsi, 2011; Yuan & Zhong, 2008) and teaching [ethical] hacking techniques has become a vital component of programs that aim to produce competent information security professionals (Dornseif, Gärtner, Holz, & Mink, 2005; Mink & Freiling, 2006).

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

The work is organized as follows: Section 2 presents the motivation for teaching offensive techniques. Section 3 presents case of teaching offensive techniques in hands-on lab exercises and the expected learning outcomes resulting from this learning and teaching approach. Sections 4 and 5 discuss the risks arising from teaching offensive techniques in an academic environment, the associated ethical concerns, and the emerging liability issues. Section 6 includes a framework for teaching these techniques Finally, Section 7 summarizes the results and conclusion.

OFFENSIVE SKILLS: WHY SHOULD THEY BE TAUGHT?

Teaching offensive skills brings a group of benefits to information security education. First, a good knowledge of offensive skills provides a perspective from the attackers' view, which better prepares students with mindsets for preventing future attacks. Second, the exposed security vulnerabilities of a target system under attack lead to deeper understanding of the security mechanism for the system. Last