

*Approaches to Ethical Hacking:*

*Expanding Conceptual Frameworks for Research*

Lauren E. Provost, Ph.D.

Rebecca Labitt

Danielle Alexandre

Asher Rodriguez

Simmons University

Abstract

The ever-changing digital landscape remains more vulnerable than ever with cybersecurity becoming increasingly important to the success of the digital economy and its stakeholders. With models including cloud computing, mobility and IoT systems, understanding how tools and methodologies for security testing have evolved is an important task. In particular, more sophisticated approaches to vulnerability assessment are currently used and necessary to address more complex security vulnerabilities. One of the central tools used in vulnerability testing is penetration testing, along with other techniques that are more broadly classified as ethical hacking. This study addresses the following research questions. (1) What are the current research trends including, current terminology and concepts, used in ethical hacking? (2) What are current challenges and best practices in ethical hacking? (3) In our multiple case-study, how do these findings relate to each case of our three industry case studies in ethical hacking?

We began by conducting a systematic review of 112 articles of peer-reviewed journals, conference proceedings and edited books from the time period of 2012-2019 to address these questions. We ranked the techniques presented in the 42 papers, a subset of the original set, based on theoretical merits, transparency of information and additional strict inclusion/exclusion criteria. Next, we provide an analysis of current research in the field including application scenarios, models, methodologies and tools. This included the completion of a literature review that includes a conceptual analysis of current terminology used in ethical hacking, both in research and in practice. We then summarize our analysis, findings and suggestions for improvements in conceptual frameworks for research in this area. Lastly, we used our resulting conceptual framework in a multi-case study approach to three ethical hacking cases for three industry participants. These results include details of the ethical hacking process in each case.

In concluding our study, we argue that current frameworks for research are limited in scope and unable to address the complexity of ethical hacking within complex cybersecurity ecosystems. The result of the literature review and multiple-case study research is an improved framework for research that encompasses a multitude of factors and attributes of major attacks that threaten computer security; a more robust, integrative multi-layered framework embracing the complexity of cybersecurity ecosystems.