

Building a Conceptual Framework For Ethical Hacking

SIMMONS UNIVERSITY, BOSTON

REBECCA LABITT

ASHER RODRIGUEZ

DANIELLE ALEXANDRE

“Complexity is the worst enemy of security, and our systems are getting more complex all the time.”

— BRUCE SCHNEIER, FROM DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD



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) What are the current conceptual frameworks for ethical hacking in research?

(3) In our multiple case-study, how do use our findings to create a robust, multi-layered framework to conceptualize and study ethical hacking?



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 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 as ethical hacking.

INTRODUCTION



Methods

-- Systemic review of 112 articles of peer-reviewed journals, conference proceedings and edited books from the time period of 2012-2019.

-- Ranked the techniques presented in the 42 papers based on theoretical merits, transparency of information and additional strict inclusion/exclusion criteria.

-- Categorized application scenarios, models, methodologies and tools as well as current terminology.

-- Used exploratory factor analysis for initial categories.



Findings

-- Current frameworks for research are limited in scope and unable to address the complexity of ethical hacking within complex cybersecurity ecosystems.

-- We made suggestions for an improved framework for research that encompasses a multitude of factors and attributes of major attacks that threaten computer security.

-- Applications of our framework to our 9 industry case studies allowed for a more robust, integrative multi-layered framework embracing the complexity of cybersecurity ecosystems.

-- Other key findings

