Approaches to Ethical Hacking: Expanding Conceptual Frameworks for Research

Danielle Alexandre
Danielle.Alexandre@Simmons.edu
Simmons University
Boston, Massachusetts

Rebecca Labitt
Rebecca.Labitt@Simmons.edu
Simmons University
Boston, Massachusetts

Asher Rodriguez
Asher.Rodriguez@Simmons.edu
Simmons University
Boston, Massachusetts

ABSTRACT

The ever-changing digital landscape remains more vulnerable than ever. Cybersecurity has become increasingly important to the success of the global, digital economy and its stakeholders. With increasing use of models such as cloud computing, mobile computing and IoT systems, understanding how tools and methodologies for security testing have evolved is an important task[1]. In particular, more sophisticated approaches to vulnerability assessment are necessary to address more complex, integrated systems. One of the central tools in addressing security vulnerabilities is penetration testing, along with other techniques that are more broadly classified as ethical hacking[2]. This study addresses the following research questions: (1) What are the current research trends, terminology and concepts used in ethical hacking? (2) What are current challenges and best practices in ethical hacking? (3) How do these findings frame an improved conceptual research for ethical hacking when applied to our three industry ethical hacking case studies? As a result of this study, we provide 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. Lastly, we use our resulting conceptual framework in a multi-case study approach to three ethical hacking cases.

CCS CONCEPTS

• **Networks** → **Network security**; *Penetration testing*; • **Cloud computing** → Dockets and containers; • **Ethical Hacking** → social engineering.

KEYWORDS

ethical hacking, network security, penetration testing, cloud security, social engineering

ACM Reference Format:
Danielle Alexandre, Rebecca Labitt, and Asher Rodriguez. 2018. Approaches to Ethical Hacking: Expanding Conceptual Frameworks for Research . In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/1122445.1122456

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Organizations and their external digital interactions leave many open possibilities for malicious attacks especially with the increase of mobile and cloud computing and IoT systems[3]. In the presence of the seemingly inexorable increase in cyber-attacks, organizations are continuously reevaluating their resiliency to a diverse set of possible threats. One approach has been to attempt to replicate the methodologies and techniques of both internal and external malicious attackers[4]. Many of these techniques have been successful, including penetration testing, along with other techniques that are more broadly classified as ethical hacking[5]. This study addresses the following research questions: (1) What are the current research trends, terminology and concepts used in ethical hacking? (2) What are current challenges and best practices in ethical hacking? (3) How do these findings frame an improved conceptual research for ethical hacking when applied to our three industry ethical hacking case studies?

We began by conducting a systematic review of 187 articles from peer-reviewed journals, conference proceedings and edited books from the time period of 2010-2019 to address the research questions. We classified the research articles systematically resulting in 46 papers, a subset of the original set. The selection criteria was based on theoretical merits, transparency of information and an additional strict inclusion/exclusion criteria. Next, we provided an analysis of current research in the field including application scenarios, models, methodologies and tools related to penetration and more broadly, ethical hacking. This included a conceptual analysis of current terminology used in ethical hacking, both in research and in practice. We then summarize our analyses, findings and suggestions for improvements, resulting in a 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. The results of the study 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.

2 OVERVIEW OF RESEARCH METHODS

2.1 Literature Review

In this paper, we considered different methods and contexts of penetration testing including tools, attack methodologies, and defense

strategies as well as additional areas classified as ethical hacking. We reviewed 187 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 46 papers, a subset of the original set, based on theoretical merits, transparency of information and additional strict inclusion/exclusion criteria. The literature review provided the necessary tools to enhance our conceptual framework that we then applied in each of our three ethical hacking case studies with three distinct organizations.

2.2 Process of Ethical Hacking and Case Study Examples

In our poster session, we will describe details of each case study, commonalities between the cases and note differences. In each case, we began in a similar way to other penetration testing methodologies[6]. At the start of the case, we collaboratively set the scope of the ethical hacking case and vulnerability assessment and goals[7]. We then began information gathering and classification of systems and technologies within scope, including relevant assets and specific situations when social engineering was used[8]. This process occurs through multiple iterations including ongoing communication with the organization for clarity on scope.

We then began reconnaissance, gathering more information about target areas within the scope of the case[9]. Scanning and access then occurred. Each case finished with an assessment of relative vulnerabilities and associated risk. The results were reported to the organizations with specific suggestions for risk management. Our poster will include specific details of different penetration techniques, socially engineered attacks and other ethical hacking techniques including, but not limited to, network service tests, DNS attacks, stateful analysis testing, socially engineered testing[10], cloud penetration testing specific to containers among others.

3 REFERENCES

[1]Tang A. (2004). A guide to penetration testing Network Security, pp. 8-14.
[2]Pfleeger, C.P., Pfleeger, S.L. & Theofanos, M.F. (1990). A methodology for penetration testing. Computer Security, 8(7), pp. 613-620.
[3]Hardy, H. (1997). The relevance of penetration testing to corporate network security. Information Security, 2(3), pp. 80-86.
[4]Smith, B., Yurcik, W. & Doss, D. Ethical hacking: The Security Justification edux. Retrieved on June 21, 2006. http://searchsecurity.com/. IEEE 2002 international symposium on technology and society (ISTAS'02), IEEE (2002), pp. 374-379.
[5]Bishop, M. (2007) "About Penetration Testing," IEEE Security Privacy, November/December 2007, pp. 84-87.
[6]Xynos, K, Sutherland, I., Read, H., Everitt, A. (2010). Penetration testing and vulnerability assessments: a professional approach. International cyber resilience conference, p. 126–32.
[7]Palmer, Charles (April, 2001). Ethical Hacking. Retrieved on June 20, 2006 from http://www.research.ibm.com.
[8]Bernard, Allen (2004). The Pros & Cons of ethical hacking. Retrieved on June 25, 2006.
[9]Beaver, Kevin. (2003). Ethical hacking: Ten crucial lessons. Information Security, 2(3), pp. 80-86.
[10] Greene, Tim (July 2004). Training Ethical Hackers: Training the Enemy? Accessed July 5, 2006 from www.ebcvg.com.
–R. LaBarge and T. McGuire, "Cloud penetration testing," Int. J. Cloud Comput., Services Archit., vol. 2, pp. 43–62, Jan. 2013.
[11]Arkin, B., Stender, S., and McGraw, G. "Software Penetration Testing," IEEE Security Privacy, January/Feburary 2005, pp. 32-35.
[12]Felter, W., Ferreira, A., Rajamony, R., and Rubio, J. (2015). An updated performance comparison of virtual machines and linux containers. In IEEE Intl Symposium On Performance Analysis of Systems and Software (ISPASS), pages 171–172.
[13]Ekici, E. (2014). Microservices Architecture, Containers and Docker. Retrieved May 1, 2018 from https://www.ibm.com/developerworks/commu
[14]Fernandez, E.B., Yoshioka, N., Washizaki, H. & Syed, M.H. (2016). Modeling and security in cloud ecosystems. Computer Security, 8(2), 13.
[15]Bernard, Allen (2004). The Pros & Cons of ethical hacking. Retrieved on June 25, 2006.
[16]Yeo, J. (2013). Using penetration testing to enhance your company's security. Computer Fraud Security, pp. 17-20.
[17]J. Zhao, W. Shang, M. Wan, and P. Zeng, "Penetration testing automation assessment method based on rule tree," in Proc. IEEE Int. Conf. CyberTechnol. Automat., Control, Intell. Syst. (CYBER), Shenyang, China, Jun. 2015, pp. 1829–1833.