

Thesis Project Portfolio

Artificial Intelligence in Cybersecurity: Impact on Penetration Testing

(Technical Report)

An Investigation into Artificial Intelligence and Automation within Penetration Testing and Cybersecurity

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Robert Mustacchio

Spring, 2023

Department of Computer Science

Introduction

Both my STS research and technical research pertain to the new technology of AI-based penetration testing. My technical capstone research is focused on the technical comparisons between this new technology and the traditional method of penetration testing which is conducted by cybersecurity professionals. My STS research focused on the potential security concerns and questions and potential ethical implications of this new technology.

Project Summaries

The goal of my technical capstone research was to investigate the capabilities of this new penetration test technology and ultimately provide a comparison between it and the traditional method of penetration testing. Specifically, my research addresses the differences between the two methods of penetration testing in terms of effectiveness, the penetration test process, and highlights any benefits or drawbacks that the AI-based penetration tests have when compared to traditional penetration tests. As these AI-based penetration tests have just recently been introduced in the penetration test market, this research gives a valuable resource for deciding ultimately what penetration test methodology should be selected for an organization's cybersecurity needs.

In my STS research, I investigated multiple potential security and ethical concerns, questions, and implications that could relate to this new technology, as there has been virtually no scholarly literature or sources within the field that address these topics. Specific concerns or questions that relate to malicious use, privacy violations or issues that could arise, and more were discussed, and their validity and severity were evaluated. My research ultimately outlines the need for further investigation and analysis of the topics of security and ethics as they relate to this technology by cybersecurity professionals.

Conclusion

As I worked on both my technical and STS research projects, each project aided my research of the other. As I would investigate the technical comparisons between traditional and AI-based penetration tests, I would encounter potential security and ethical topics that could be addressed in my STS research, and likewise, as I explored various ethical and security topics for my STS research, I came across various potential benefits or drawbacks associated with method of penetration testing over the other. Overall, I believe that both my technical and STS research provide a valuable resource in evaluating the new technology of AI-based penetration testing. Through my research, one can gain understanding of this new technology and its technical comparisons to traditional penetration testing, as well as new perspectives regarding the security and ethical topics that could arise and need to be addressed by professionals within the field.

Lastly, I would like to acknowledge my STS professor, Professor Richard Jacques, as well as my capstone instructor, Rosanne Vrugtman, and thank them for their assistance.

Table of Contents

Sociotechnical Synthesis

Artificial Intelligence in Cybersecurity: Impact on Penetration Testing

An Investigation into Artificial Intelligence and Automation within Penetration Testing and Cybersecurity

Prospectus