# Artificial Intelligence in Cybersecurity: Impact on Penetration Testing

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

**Robert Mustacchio**

Spring, 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Rosanne Vrugtman, Department of Computer Science

# Artificial Intelligence in Cybersecurity: Impact on Penetration Testing

CS4991 Capstone Report, 2023

Robert Mustacchio
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
rmm6ts@virginia.edu

## ABSTRACT

A southern U.S. cybersecurity firm that provides services to over 2,500 customers wanted to expand its consumer base by providing penetration test services to new markets. To help with this, I researched various major players in a variety of penetration test markets to look for holes in their offerings, new technology and methods, and openings for this firm to exploit. I utilized every possible resource including company websites and white papers, scholarly papers and articles available to students, and open-source penetration test solutions and services. I compiled all of the necessary information including market information and specific penetration test offerings, pricing, and how certain penetration test solutions worked. I then presented my findings to the executive team at this firm, which they used to inform and influence their decisions about market expansion and potential service/solution development. One byproduct of my research was the discovery of penetration test solutions and services that utilized artificial intelligence, from solutions that automated some components of the penetration test process to solutions that were fully automated. Although not required for this firm, some follow-up research that more closely inspected and analyzed these artificial intelligence solutions could be very beneficial to the fields of cybersecurity and artificial intelligence.

## 1. INTRODUCTION

Over the past several years, it has become dramatically important to ensure the safety and security of sensitive information and data. As technology continues to advance, so do the resources and methods that cyber criminals use to attempt to exploit vulnerabilities and steal sensitive information from individuals and organizations. These cyber criminals can carry out attacks that result in substantial damage in several different ways, including financial damages and leaks of sensitive and confidential information and data. Because of this, it is imperative that strong cybersecurity measures and practices are in place to be able to protect against these cyber-attacks.

## 2. RELATED WORKS

While the utilization of AI within the penetration testing and overall cybersecurity field is relatively new, various published works that dive into this subject have aided me in my research.

A paper by Stefinko, et al, (2016) addresses the differences and similarities between manual and automated penetration testing. They also touch on the benefits, drawbacks, and associated concerns with the trend of the penetration testing market becoming increasingly automated. A paper by Garrad and Unnnikrishnan (2022) details the use and benefit of AI in penetration testing of a connected and autonomous vehicle network.

Their real-world applications and data provide insight into how developed these automated pen test solutions are as well as their current effectiveness. Another major related work that influenced my research is a paper by Abu-Dabaseh and Alshammari (2022). Their work gives a general overview of automated penetration testing, how it measures up to manual penetration testing, and the current automated penetration testing landscape.

## 3. PROCESS DESIGN

One of the most popular methods that companies and organizations utilize to keep their information safe and secure is penetration testing. Penetration testing, sometimes referred to as ethical hacking or pen testing, is a security measure in which the testers mimic real-world attacks on a system to identify any vulnerabilities. Pen tests can be performed on applications, networks, employees or members of a company or organization, and other system components. The pen test process usually consists of a vulnerability scan, simulated attacks, and then analysis and reporting of any vulnerabilities that were found and exploited. Overall, pen testing is an effective way to maintain and strengthen an organization's cybersecurity and is essential in fighting against cyber-attacks.

Recently, the use of artificial intelligence (AI) in penetration testing has emerged as a promising solution to improve the efficiency of pen tests. Cybersecurity firms are starting to utilize AI to automate certain parts of the pen test process to even being able to perform entire pen tests autonomously. This is exciting because of the various benefits that automated pen tests would provide, such as being far less labor-intensive and costly than traditional pen tests, and also enabling security experts to focus their time on preemptive security measures. However, there is some concern within the field about the rise of AI in pen testing because there are still bugs that need to be worked out in terms of system compatibility with these automated solutions and the tendency of these automated solutions to produce false positives that end up wasting the organization's time and resources.

From February to July of 2022, I interned for a southern U.S. cybersecurity firm that provides services to over 2,500 customers. My main project with this firm was to help the executive team determine if the firm could broaden its market reach, specifically within the pen test market. To do this, I first got an in-depth look at the firm's pen test offerings, including the specific types of pen tests, pricing, and pen test timeline. I then spent the next few months researching the pen test offerings of a number of selected cybersecurity firms by the executive team of the firm.

## 4. RESULTS

At the end of my research, I prepared a presentation for the executive team that contained all of my findings about the pen test market, the pen test offerings of the firms that they gave me, as well as any apparent gaps within the pen test market that they firm could pursue and my recommendation on what gaps would be the most beneficial to pursue.

What I found was that the fastest growing parts of the pen test market were the Education, Retail, and Healthcare sectors and I recommended that the firm start marketing and tailoring their offerings to customers within those areas. I also found that the new trend within the pen test market was automated pen tests and recommended that the firm look into those capabilities. The rest of my research was a deep dive into how these automated pen tests work and the benefits and drawbacks that they posed.

In a manual pen test, every component of the pen test process is performed by a cybersecurity professional, including the vulnerability assessment, exploit development and management, reporting, and cleanup. This causes manual pen tests to be very time-consuming, costly, and difficult to repeat. On the other hand, with the utilization of AI, all of these components can be either fully or semi-automated. It is also shown that these automated solutions have nearly the same capabilities as manual ones meaning that the automated tests can be performed on most systems and test most components of an organization's system, network, or application.

This is an exciting development within the cybersecurity field because making these pen tests less capital- and time-intensive would make them far more accessible and would reduce the time and labor for the professionals that need to perform the manual tests. However, these automated tests are certainly not rid of any flaws or drawbacks. One of the main concerns is that these automated pen tests may not be as effective as the human-driven pen tests as it is unknown as to if they are able to identify more complex vulnerabilities or simulate more advanced attack scenarios. Automated pen tests also have a habit of producing false positives or false negatives, which lead to professionals either searching for a vulnerability that is not there or completing missing a vulnerability that is there. Another drawback is that the automated tests require much more significant configuration and tuning to ensure that they can be performed on an organization's specific system and security requirements. Finally, these automated tests may not be able to fully replace manual tests because human expertise is still needed to perform tests on areas such as social engineering and physical security testing.

## 5. CONCLUSION

My internship with a southern U.S. cybersecurity firm was a valuable experience that allowed me to learn and gain experience in both business and cybersecurity. Specifically, I had the opportunity to learn about penetration testing, a critical process for assessing and strengthening the cybersecurity of an organization. This experience sparked my interest in the topic, leading me to further research, specifically the new AI-based penetration testing solutions that firms were starting to develop and release.

Through this research, I discovered that while automated penetration testing solutions certainly have a number of advantages over traditional manual testing, they are not yet a complete replacement for human expertise. Automated solutions can quickly and efficiently identify potential vulnerabilities in a system, and do it for much cheaper, but they are currently limited by their ability to detect complex vulnerabilities that require human expertise and experience. Additionally, manual penetration tests offer a more holistic approach, allowing testers to search for more kinds of vulnerabilities and identify potential gaps or issues that automated solutions may overlook.

Overall, my research into automated penetration testing solutions was beneficial to the field of cybersecurity as it highlighted some of the advantages of this technology as well as some of the drawbacks and components that need to be further developed and improved. As this technology continues to advance and become more prevalent in the industry, it is important for organizations to be aware of the capabilities and limitations of these solutions in order to make informed decisions about their cybersecurity needs and strategies.

## 6. FUTURE WORK

While I believe my research was beneficial to the penetration testing and cybersecurity industry as a whole because it provided valuable insights into the current capabilities and limitations of automated penetration testing solutions, there is still much work to be done in this field. As this technology continues to advance and evolve, it is important to conduct further research to understand their effectiveness compared to traditional testing methods. Specifically, there is a need for more investigation into specific automated solutions and how they stack up against a traditional penetration test process in order to determine which approach is most effective in different scenarios. This could include experimentation with several different automated tools on various different types of penetration tests and comparing their results with those of a human tester's process.

Additionally, as automated penetration testing solutions are a relatively new development in the field, there is currently no long-term research or analysis concerning their effectiveness. It is essential to continue monitoring the performance of these automated solutions over time so that we can better understand their long-term impact to an organization's cybersecurity and make more informed decisions pertaining to their use. Ultimately, continued investigation into automated penetration testing solutions will be critical to improving the overall cybersecurity of organizations and protecting against emerging and evolving cybersecurity threats.

## REFERENCES

[1] Farah Abu-Dabaseh and Esraa Alshammari. (n.d.) *Automated Penetration Testing: An Overview*. https://airccj.org/CSCP/vol8/csit88610.pdf

[2] Philip Garrad and Saritha Unnikrishnan. (n.d.) *Artificial Intelligence in Penetration Testing of a Connected and Autonomous Vehicle Network*. https://www.researchgate.net/profile/Saritha-Unnikrishnan/publication/361293660_Artificial_Intelligence_in_Penetration_Testing_of_a_Connected_and_Autonomous_Vehicle_Network/links/638e1e6811e9f00cda1f2ce0/Artificial-Intelligence-in-Penetration-Testing-of-a-Connected-and-Autonomous-Vehicle-Network.pdf

[3] Yaroslav Stefinko, Andrian Piskozub, and Roman Banakh. 2016. *Manual and automated penetration testing. Benefits and drawbacks. Modern tendency*. DOI:https://doi.org/10.1109/TCSET.2016.7452095