Utilization of Artificial Intelligence and Automation in Penetration Testing and Vulnerability Scanning

(Technical Paper)

Advantages, Risks, and Threats Associated with Increased Automation in Cybersecurity

(STS Paper)

A Thesis Prospectus Submitted to the

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

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

Robert Mustacchio

Fall, 2022

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

STS Advisor: Richard D. Jacques, Ph.D., Department of Engineering & Society

Introduction

In recent years, society has become increasingly dependent on technology within every facet of life, especially so in the modern business landscape. This elevated reliance on technology for business has led to organizations' heightened commitment to cybersecurity. One of the most common ways that organizations maintain and strengthen their cybersecurity is through the utilization of penetration testing. Penetration testing, sometimes referred to as ethical hacking, is the process of identifying vulnerabilities within a security system and exploiting them to understanding the level of threat they pose and the damages that would be caused by an attack (Keshri, 2022). Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weakness in a system (Ridge Security Marketing, 2021). There are several types of penetration tests, the most prevalent being web and mobile application, network, and social engineering penetration tests. Penetration testing is incredibly important because it allows an organization to evaluate its ability to protect its networks, applications, endpoints and users from external or internal attempts to circumvent its security controls and gain unauthorized or privileged access to protected assets (CoreSecurity, 2022).

For decades, penetration testing had been performed exclusively by teams of ethical hackers. However, due to its labor-intensive and costly nature, there has been a recent push for more automated methods. This has led to an emergence of semi-automated and fully automated penetration testing solutions in the market, with several companies now working on and offering these automated solutions. The technical topic area of this prospectus is my experience during my cybersecurity internship as well as further exploration of these pentesting processes that employ automation and artificial intelligence with regards to how they work. This prospectus will also feature an STS discussion of the advantages and disadvantages of these automated

penetration test solutions as well as the security and ethical concerns with increased automation in the field of cybersecurity.

Utilization of Artificial Intelligence and Automation in Penetration Testing and Vulnerability Scanning

From February to August of 2022, I was a Cybersecurity Intern for a leading cybersecurity company that primarily provides services to financial institutions. Throughout the duration of my internship, I completed multiple projects and learned a great amount of valuable information, methods, and techniques with regard to cybersecurity, technical writing, research, and business. One of the projects I completed for this internship involved thorough research on a number of competing cybersecurity firms and their penetration test offerings. It was during this research that I was introduced to "automated penetration test solutions", which had started to surface in the market in recent years. The rest of the technical portion of this prospectus will further explore both manual and automated penetration tests and will dive into how they work and if there exists any opportunities within the cybersecurity market as a whole for further automation.

As stated above, penetration testing involves identifying vulnerabilities within a system and then exploiting them to understand the level of threat they pose to an organization. Within the field, this process is occasionally treated as two separate processes, with vulnerability scanning being the process of identifying the vulnerabilities, and penetration testing being the process of exploiting those vulnerabilities. For the purposes of this prospectus and since penetration testing and vulnerability scanning are almost always performed in tandem, each of these processes will be considered portions of a penetration test. For decades, manual penetration

testing was the only option for organizations to evaluate the security of their systems. The hired security experts would perform every component of a penetration test manually, including data collection, conducting a vulnerability assessment, exploiting the detected vulnerabilities, and then preparing a report on the system including security recommendations (TutorialsPoint, 2022). In recent years, manual penetration testing has now included some form of automation because the security experts involved now use automated tools such as Kali Linux, nmap, and Metasploit that help with the data collection and vulnerability assessment portions of a manual penetration test (Nesbo, 2022). The human tester then manually exploits the system's vulnerabilities and then prepares a report that describes the vulnerabilities and recommends corrective steps to protect the system.

As advancements have been made in the field of artificial intelligence and automation, it is slowly being incorporated into every aspect of life and business with cybersecurity being no exception. The cybersecurity market is now seeing companies starting to offer their own version of automated penetration testing that employ automation and/or artificial intelligence. These "automated penetration tests" as they're being marketed range from hybrid approaches that combine human ethical hackers with proprietary automated systems that perform vulnerability checks on the target system to fully automated tools that perform entire penetration tests. In the case of the hybrid solutions, the automated tools continuously check the system for any vulnerabilities, and when vulnerabilities are found, security experts are alerted and they run more sophisticated checks before trying to exploit the discovered vulnerability. This type of approach has become very popular, with dozens of companies creating their own automated vulnerability scanners and marketing their hybrid approach. The fully automated penetration test solutions employ the use of artificial intelligence that gathers data about the target system and then

performs entire penetration tests on its own. This is currently far less popular, with one of the main examples of this being Deep Exploit, an open-source fully automated penetration testing tool that uses machine learning (Son, 2022).

It seems that the clear direction of the penetration testing market is these automated solutions becoming the new norm, which begs the question of where in the cybersecurity market should automation be introduced next. There have already been several suggestions by cybersecurity experts themselves as to which areas should shift to artificial intelligence and machine learning next, the most popular being generating protections faster than attacks can spread and detecting infections already within a network (Palo Alto Networks, 2022). As more and more advancements are made within the fields of artificial intelligence and automation, it will be interesting to witness just how much support they can provide in regard to cybersecurity for modern organizations.

Advantages, Risks, and Threats Associated with Increased Automation in Cybersecurity

With regards to the effectiveness of penetration testing, automated solutions have many advantages and drawbacks compared to the traditional, fully manual solutions. First, automated penetration test solutions are significantly cheaper than manual penetration tests because instead of hiring a security expert, an organization would just have to pay for the software and run it on their system. The relatively lower costs of the automated solutions also make them much more repeatable, allowing organizations to run them regularly and thus have a higher chance of discovering a vulnerability quickly. Automated penetration test solutions can also discover identical or nearly identical problems as a hired penetration tester (Nesbo, 2022). This means that smaller organizations and businesses that may not have the resources to afford hiring a team of security experts to come in and test their system can still make their system and data secure.

However, there are many areas in which automated penetration testing fails to meet the capabilities of a team of manual penetration testers. For instance, it is much easier for a team of manual penetration testers to think like an attacker, and thus come up with more ways of hacking a system than an automated tool can (Nesbo, 2022). Another reason automated penetration testing tools may not be as effective as manual tests is that some organizations' systems may not be compatible with online tools, meaning that in terms of performing tests, they are not nearly as accessible. Automated penetration test solutions also have a habit of producing false positives and reporting a vulnerability when there actually isn't one, which results in wasted time and effort (EasyDmarc, 2022).

There are ethical concerns with these automated solutions as well, notably the threat of job displacement of security experts as more and more fully automated solutions come to market. There are arguments that these automated tools actually help these security experts because it relieves them of having to worry about testing and surveillance and allows them to focus on more preemptive security measures. However, with the trend of the increase of automated tools in the field, it seems as though this could be just the beginning of security professionals' functions being eaten away at.

It is estimated that by 2025, the market for artificial intelligence for cybersecurity tasks will grow to $34.8 billion (Taddeo, M., McCutcheon, T., & Floridi, L., 2019). As modern society becomes more reliant on artificial intelligence, machine learning, and automation, the more critical it is that proper attention is given to mitigating the risks and threats associated with these fields, especially with respect to cybersecurity. While the use of artificial intelligence and automation for cybersecurity surely has a great amount of potential for good, it also introduces a whole new way for attackers to wreak havoc. Cybercriminals are already weaponizing artificial

intelligence to conduct cyberattacks, and now with the increased utilization of automated tools and artificial intelligence for security, it won't be long until cybercriminals start attempting to weaponize those (Gregory, 2021). For example, some of the current automated penetration testing tools mentioned above are designed to search for vulnerabilities and notify a security professional when one is found. With current tools, a cybercriminal could breach the target organization's system, mimic the automated security tool, and wreak havoc within the system. The use of artificial intelligence in cybersecurity also brings upon a set of generic concerns about artificial intelligence like biases, incorrect tendencies, and data poisoning. It is crucial that proper attention is given to these concerns so that this increase of automation and artificial intelligence within cybersecurity has its benefits greatly outweigh its drawbacks.

Conclusion

Through my internship I was introduced to the growing level of dependence upon automation and artificial intelligence for cybersecurity process and practices. After further research on the capabilities of these tools, it is clear that the dependence for them will only continue to grow in the field of cybersecurity. However, as stated above, there are a number of concerns, both in regards to security and ethics, that must be appropriately handled to ensure that they do in fact increase our society's level of security, rather than providing yet another way in which cybercriminals can inflict harm.

Word Count: 1721

References

CoreSecurity. (2022). *Penetration Testing: Breaking in to Keep Others Out*. Penetration Testing: Breaking in to Keep Others Out | Core Security Blog. Retrieved October 20, 2022, from https://www.coresecurity.com/blog/penetration-testing-breaking-keep-others-out

EasyDmarc. (2022, May 6). *Automated penetration testing VS. manual penetration testing*. EasyDMARC. Retrieved October 26, 2022, from https://easydmarc.com/blog/automated-penetration-testing-vs-manual-penetration-testing/

Gregory, J. (2022, July 5). *AI security threats: The real risk behind science fiction scenarios*. Security Intelligence. Retrieved October 23, 2022, from https://securityintelligence.com/articles/ai-security-threats-risk/

Keshri, A. (2022, October 10). *What is Automated Penetration Testing? Difference Between Automatic & Manual Pentesting*. Astra Security Blog. Retrieved October 24, 2022, from https://www.getastra.com/blog/security-audit/automated-penetration-testing/#:~:text=Automated%20penetration%20testing%20or%20Vulnerability,performed%20by%20competent%20security%20researchers.

Nesbo, E. (2022, June 27). *Manual vs. Automated Penetration Testing: What's the Difference?* MUO. Retrieved October 26, 2022, from https://www.makeuseof.com/manual-vs-automated-pen-testing/

Palo Alto Networks. (2022). *4 Ways Cybersecurity Automation Should be Used*. Palo Alto Networks. Retrieved October 26, 2022, from

https://www.paloaltonetworks.com/cyberpedia/4-ways-cybersecurity-automation-should-be-used

Ridge Security Marketing. (2021, July 15). *The Past, Present, and Future of Pentesting*. Ridge Security. Retrieved October 20, 2022, from https://ridgesecurity.ai/blog/the-past-present-and-future-of-pentesting/

Son, D. (2020, May 9). *Deep Exploit: Fully Automatic Penetration Test Tool Using Machine Learning*. Penetration Testing. Retrieved October 26, 2022, from https://securityonline.info/deep-exploit/

Taddeo, M., McCutcheon, T., & Floridi, L. (2019, November 11). *Trusting artificial intelligence in cybersecurity is a double-edged sword*. Nature News. Retrieved October 31, 2022, from https://www.nature.com/articles/s42256-019-0109-1#citeas

TutorialsPoint. (2022). *Penetration Testing - Manual & Automated*. Tutorials Point. Retrieved October 26, 2022, from https://www.tutorialspoint.com/penetration_testing/penetration_testing_manual_automated.htm#:~:text=The%20only%20difference%20between%20them,is%20done%20by%20machine%20itself.