ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 10, No. 1, 2025

ARTIFICIAL INTELLIGENCE IN PENETRATION TESTING: LEVERAGING AI FOR ADVANCED VULNERABILITY DETECTION AND EXPLOITATION

Mariia Kozlovska[1], Andrian Piskozub[1], Volodymyr Khoma[2]

[1] *Lviv Polytechnic National University, 12, S. Bandery str., Lviv, 79013, Ukraine,*
[2] *Opole University of Technology, 76, Proszkowska str., Opole, 45758, Poland*
Authors' e-mails: *mariia.kozlovska.kb.2021@lpnu.ua, andriian.z.piskozub@lpnu.ua, v.khoma@po.edu.pl*

https://doi.org/10.23939/acps2025.01.065

Submitted on 12.04.2025

***Abstract*: The article examines the ways artificial intelligence is influencing the penetration testing procedure. As technology advances and cyber threats grow more common, conventional testing methods are insufficient. Artificial intelligence aids in automating processes like vulnerability detection and real-world attack simulation, leading to quicker, more precise results with reduced dependence on human input. Machine learning is a game-changer in identifying hidden security flaws by analyzing past attacks and abnormal patterns. Tools mentioned in the article are revolutionizing vulnerability detection, traffic monitoring, and attack simulations. These tools have better key performance metrics, such as scan time, false positive rate, detection accuracy, mean time to detect, zero-day threats / month, compared to traditional penetration testing tools.**

***Index terms*: artificial intelligence, penetration testing, vulnerability detection, cybersecurity, machine learning.**

I. INTRODUCTION

In the current digital age, cyberattacks are becoming more common, advanced, and challenging to identify. These assaults aim at companies, institutions, and people, frequently leading to data leaks, monetary losses, and harm to reputations. With the increasing frequency and sophistication of cyber threats, organizations of every size are making substantial investments in advanced cybersecurity tools and services to protect their data and IT systems. One of the key practices in this domain is penetration testing, a technique employed to assess the security of IT systems by mimicking actual cyberattacks to uncover possible weaknesses that could be targeted by harmful entities [1].

Traditionally, penetration testing has been performed manually by exceptionally talented cybersecurity experts. These professionals depend on their expertise, established protocols, and a range of specialized testing instruments to identify vulnerabilities in a system's security. Yet, as information technology settings keep advancing and growing in complexity, conventional approaches to penetration testing are starting to reveal shortcomings. Manual testing can be time-consuming, subject to human mistakes, and, crucially, might not consistently reveal deeper, more complex vulnerabilities, particularly in large or frequently evolving systems [2].

This is the point at which artificial intelligence becomes relevant. Through the incorporation of artificial intelligence in penetration testing procedures, it is now feasible to automate many tedious and repetitive tasks that were once performed by human testers. This integration facilitates the examination of large data volumes in a significantly shorter time than what a human tester would require, allowing for quicker and more precise detection of vulnerabilities. Additionally, artificial intelligence is capable of mimicking the actions of cyber attackers with greater realism, enhancing the overall efficiency of testing methods. Machine learning, which is a branch of artificial intelligence, is essential for automating the identification of vulnerabilities and their exploitation in penetration testing [3].

Machine learning algorithms can examine past attack information and recognize unusual patterns in system behavior, which aids in uncovering potential security vulnerabilities that might be overlooked by conventional techniques. Additionally, deep learning methods can improve this process by analyzing intricate data frameworks and revealing weaknesses that necessitate more sophisticated analytical skills [4].

Artificial intelligence aids in the management and analysis of technical documents associated with security evaluations. Natural language processing allows systems to derive insights from substantial amounts of text, including technical reports or code evaluations, improving documentation and decision-making in penetration testing. Although there are advantages, obstacles persist, such as grasping how artificial intelligence systems arrive at decisions and their flexibility in different IT settings.

Nonetheless, integrating artificial intelligence into penetration testing greatly boosts the effectiveness and precision of cybersecurity initiatives, allowing for quicker threat identification, fewer false positives, and enhanced response durations [5]. As artificial intelligence advances, it has significant potential to independently detect and mitigate cyber threats instantly, enhancing cybersecurity measures.

II. LITERATURE REVIEW AND PROBLEM STATEMENT

The integration of Artificial Intelligence (AI) into penetration testing is an area of growing interest in

cybersecurity research, offering significant advancements in the automation and enhancement of traditional testing methods. Penetration testing is a critical practice used to assess the security of IT systems by simulating cyberattacks in order to identify potential vulnerabilities. As cyberattacks evolve in sophistication and frequency, traditional manual penetration testing is increasingly showing its limitations. AI technologies, particularly Machine Learning (ML) and Deep Learning (DL), present potential solutions to these challenges by automating repetitive tasks, identifying hidden vulnerabilities, and simulating advanced cyberattacks. This section reviews various studies and discussions around the application of AI in penetration testing, focusing on its benefits, challenges, and evolving trends.

Penetration testing has historically relied on human experts, who follow predefined protocols to identify vulnerabilities in systems. However, this process is time-consuming, prone to human error, and limited by the testers' expertise and available tools. As IT environments become more complex, traditional methods struggle to identify deep, intricate vulnerabilities, particularly in large or constantly evolving systems. In the article [6], it is emphasized that AI's ability to process large datasets and recognize hidden patterns enables more effective and timely detection of vulnerabilities, which may otherwise go unnoticed in manual testing. By analyzing past attack data, AI can predict potential vulnerabilities and simulate attacks, offering deeper insights into the system's weaknesses.

Machine Learning, a subset of AI, has been extensively explored as a tool for automating vulnerability detection. According to the article [7], ML algorithms analyze massive amounts of historical attack data to identify anomalies and patterns in system behavior, which are indicative of potential security flaws. Deep Learning enhances this further by enabling AI systems to work with more complex and higher-dimensional data, uncovering vulnerabilities that traditional methods may miss. This automation significantly improves the efficiency of penetration testing, particularly in large and dynamic IT infrastructures.

AI is also valuable in simulating real-world attacks. While traditional penetration testing involves human testers attempting to replicate cyberattacks, AI systems can simulate these attacks with greater accuracy and realism. The article [8] discusses how AI-driven tools can mimic the tactics, techniques, and procedures (TTPs) of actual cybercriminals, providing more comprehensive insights into the system's potential vulnerabilities and how they could be exploited. These simulations are particularly useful for testing advanced persistent threats (APTs) and zero-day vulnerabilities, which require sophisticated attack methods that can be difficult for human testers to replicate effectively.

In addition, AI contributes to the analysis and management of technical documentation, such as vulnerability reports, security logs, and code evaluations. The article [9] highlights the role of Natural Language Processing (NLP) in enabling AI systems to analyze large volumes of textual data and extract meaningful insights. NLP tools help automate report generation, categorize vulnerabilities, and prioritize security risks, which speeds up decision-making and enhances the overall penetration testing process.

Despite these advancements, several challenges remain in integrating AI into penetration testing. One major issue is the "black-box" nature of many AI models, which makes it difficult to understand how decisions are made. The article [10] emphasizes that this lack of transparency can be problematic in cybersecurity, where understanding the reasoning behind a finding is critical for remediation. AI models, especially deep learning models, are often viewed as opaque, making it difficult for security professionals to trust their recommendations fully. This challenge is further compounded by the need for AI systems to adapt to rapidly changing IT environments and continuously evolving threats. The article [11] addresses these concerns, highlighting the need for AI systems that can learn in real-time and adjust to new attack strategies, network configurations, and vulnerabilities.

Moreover, the integration of AI tools with existing security infrastructures remains a challenge. Many organizations continue to rely on traditional penetration testing methods, and incorporating AI into these processes requires careful planning. The article [12] stresses that AI should not replace human testers but rather complement their expertise. Combining AI's analytical power with human insight ensures a more effective and well-rounded penetration testing process.

In conclusion, artificial intelligence has the potential to greatly enhance the effectiveness and efficiency of penetration testing. By automating repetitive tasks, simulating real-world cyberattacks, and improving vulnerability detection, artificial intelligence tools can provide deeper insights into system security and help identify weaknesses more accurately and faster than traditional methods. However, issues such as model transparency, adaptability to changing environments, and integration with existing tools must be addressed to fully realize artificial intelligence's potential in penetration testing. As the field continues to evolve, artificial intelligence is likely to play an increasingly important role in cybersecurity practices, enabling more proactive, efficient, and comprehensive defense mechanisms.

III. SCOPE OF WORK AND OBJECTIVES

This study explores the growing role of artificial intelligence in penetration testing and vulnerability assessment. It focuses on how AI improves security testing procedures' automation, accuracy, and efficiency. Leading AI-powered tools are assessed, their skills are compared, and their usefulness in detecting and controlling vulnerabilities is examined in this study. While taking into account the potential of AI in cybersecurity in the future, it also looks at present issues including false positives, data dependence, and ethical issues. In addition to offering suggestions for its

successful implementation, the objective is to clearly explain how AI may complement and enhance conventional security procedures.

IV. COMPARING AI-POWERED TOOLS FOR PENETRATION TESTING AND VULNERABILITY ASSESSMENT

Artificial Intelligence (AI) is transforming the field of penetration testing, bringing new levels of efficiency, speed, and accuracy to vulnerability detection and threat analysis. By integrating AI into these tools, security professionals can automate time-consuming tasks, reduce human error, and focus on the most critical threats. AI-powered tools can quickly scan and assess systems, applications, and networks, identifying vulnerabilities with far greater precision than traditional methods. Table 1 compares key performance metrics between traditional and AI-powered penetration testing methods to highlight these improvements.

Table 1

AI vs. traditional penetration testing metrics

Metric	Traditional	AI-Powered
scan time	~24 hours	4–6 hours
false positive rate	~30 %	<5 %
detection accuracy	~85 %	>95 %
mean time to detect	~8 hours	1–2 hours
zero-day threats / month	1–2 vulnerabilities	5–7 vulnerabilities

A variety of tools have emerged that utilize AI to improve penetration testing processes, particularly in areas like vulnerability scanning, network traffic analysis, and automated exploitation. Vulnerability scanners, for instance, have become much more intelligent with AI integration. Tools like Nessus (from Tenable.io) leverage machine learning algorithms to continuously refine their detection capabilities. By analyzing historical vulnerability data, these tools learn from past patterns, which helps them predict and identify new vulnerabilities more accurately [13]. Similarly, Intruder, another vulnerability scanner, employs AI to analyze real-time threats and continuously monitor assets, offering an adaptive defense against new vulnerabilities [14].

For web applications, Acunetix combines AI with automated scanning to detect and classify vulnerabilities while minimizing false positives. AI's ability to understand complex website structures and interactions ensures that Acunetix provides more accurate findings, reducing unnecessary alerts and focusing on actionable vulnerabilities [15]. These advancements mean that security teams can spend less time verifying vulnerabilities and more time fixing them.

In the realm of network traffic analysis, AI plays a crucial role in real-time threat detection. Tools like Darktrace have pioneered the use of machine learning to monitor network traffic and detect anomalies that might signify an attack. Darktrace's AI learns from the behavior of regular network traffic and adapts in real-time, allowing it to identify unusual patterns and potential security breaches before they can cause harm [16]. Similarly, Zeek (formerly known as Bro), an open-source network monitoring tool, uses behavioral analysis to detect and log suspicious traffic, while also leveraging AI to enhance its ability to identify and respond to emerging attack vectors [17].

AI-powered intrusion detection systems, such as Snort (when enhanced with machine learning), can automatically adapt to new threats by analyzing patterns in network traffic and identifying subtle variations indicative of an attack. As the system learns from past attacks, its ability to detect and prevent future threats improves, providing a more dynamic defense mechanism [18].

Automated penetration testing tools have also seen significant advances with AI. Pentera, for example, automates vulnerability scanning and attack simulations, allowing security teams to identify weaknesses in their systems and verify their defenses in a more streamlined manner. By simulating real-world cyberattacks, Pentera provides valuable insights into how a system would withstand actual malicious attempts, making it an essential tool for continuous security testing [19].

For more sophisticated automated testing, DeepExploit takes AI-driven penetration testing a step further by fully automating the process, from discovering vulnerabilities to exploiting them. This tool is designed to replicate the actions of a skilled penetration tester, offering a thorough assessment of an organization's defenses with minimal human input. By leveraging machine learning, DeepExploit ensures that the penetration testing process is both efficient and thorough [20].

AI's role doesn't stop at detection; tools like IBM QRadar Advisor with Watson have begun integrating AI to analyze security incidents and streamline the investigative process. Watson's natural language processing capabilities enable security teams to investigate threats more quickly, reduce response times, and ultimately mitigate risks faster [21].

The integration of AI into penetration testing not only automates repetitive tasks but also enhances the accuracy and depth of vulnerability assessments. These AI-driven tools continuously learn and improve, providing security professionals with powerful insights and recommendations. By identifying vulnerabilities and simulating attacks more efficiently, organizations can stay one step ahead of cybercriminals, ultimately leading to stronger, more resilient systems.

Table 2 provides a comparison of various AI-powered tools used in penetration testing and vulnerability assessment, outlining the key technologies they utilize and their notable features that enhance security operations.

These tools not only identify vulnerabilities with precision but also provide valuable insights into how these weaknesses can be mitigated. With their ability to automate and enhance traditional penetration testing methods, AI tools are paving the way for a more robust, proactive approach to cybersecurity.

Table 2

Comparison of AI-powered tools for penetration testing and vulnerability assessment

Tool	Key Technologies	Notable Features
Tenable.io (Nessus)	Machine Learning, Risk Analysis	Advanced system configuration analysis, risk evaluation
Intruder	Machine Learning	Continuous asset monitoring, real-time threat detection
Acunetix	AI, Web Traffic Analysis	Decreased false positives, actionable remediation suggestions
Darktrace	AI, Self-Learning	Real-time anomaly detection, adaptive learning to new threats
Zeek (Bro)	Behavioral Analysis	Deep traffic analysis, anomaly detection
Snort AI-enhanced	Machine Learning	Adaptation to new threats, increased detection accuracy
Pentera	AI, Attack Simulation	Automated vulnerability scanning, attack simulations, report generation
DeepExploit	Machine Learning	Complete automation of vulnerability discovery and exploitation
IBM QRadar Advisor with Watson	AI, Natural Language Processing	Threat analysis, incident investigation, reduced response time

V. CHALLENGES AND LIMITATIONS OF AI IN PENETRATION TESTING

Despite the benefits AI-powered penetration testing tools offer in terms of efficiency and accuracy, their adoption comes with several challenges and limitations that need to be carefully addressed.

A primary concern is the occurrence of false positives and false negatives. False positives can lead to unnecessary alerts and wasted resources when a non-existent vulnerability is flagged. False negatives, on the other hand, may leave critical security gaps unaddressed. Although AI systems are continually improving, human oversight remains essential to minimize these errors and ensure the reliability of results.

Another limitation is the over-reliance on automation. While AI excels in handling repetitive tasks and processing large datasets, it lacks the intuitive decision-making and contextual understanding that human testers provide. AI should therefore be viewed as a tool to augment, not replace, human expertise. Skilled professionals remain essential for nuanced analysis and decision-making in complex security scenarios.

AI's effectiveness also depends on the quality and breadth of the data used for training. The ever-evolving threat landscape means that AI models may struggle to detect new or highly customized attack methods unless continuously updated with fresh data. Without this ongoing adaptation, AI tools may be less effective in addressing novel threats.

Ethical and legal issues also arise when deploying AI in penetration testing. Automating the testing process, especially when exploiting vulnerabilities, could lead to misuse if the tools fall into the wrong hands. Additionally, privacy concerns emerge when testing systems that handle sensitive data. Improperly executed tests may lead to data breaches or legal violations. Strong ethical guidelines and regulatory frameworks will be needed to ensure AI tools are used responsibly.

Finally, AI tools in penetration testing can be resource intensive. They require substantial computational power and skilled professionals to manage and interpret results. Smaller organizations may struggle with the high costs associated with deploying AI-driven solutions, making these tools less accessible to all.

VI. THE FUTURE OF AI IN PENETRATION TESTING AND CYBERSECURITY

The future of AI in penetration testing and cybersecurity looks bright. As AI technology advances, it will make security practices more proactive, efficient, and intelligent.

One of the most exciting developments is AI-driven threat hunting and prediction. AI's ability to analyze large data sets and detect emerging patterns will allow penetration testing tools to predict cyberattacks before they occur. This approach will help identify vulnerabilities early, allowing teams to address high-risk issues before they escalate. The shift from reactive to proactive security will significantly boost the effectiveness of penetration testing.

As machine learning models improve, AI tools will become more accurate in detecting vulnerabilities. With access to more diverse and up-to-date threat data, these systems will identify new attack methods and vulnerabilities faster, ensuring they stay ahead of evolving threats.

AI will also be integrated with threat intelligence platforms. By combining real-time threat data with AI's analytical power, penetration testing tools will adapt and respond more quickly to new risks. This will help cybersecurity teams stay ahead of attackers by refining their testing strategies based on the latest threat information.

Both offensive and defensive cyber operations stand to benefit. Red teams will utilize AI to orchestrate more realistic and intricate simulations, rigorously challenging system defenses. Meanwhile, blue teams will deploy AI to monitor and counter threats with greater precision and speed.

Although many aspects of penetration testing will be automated, human expertise will remain essential. AI's

speed and accuracy will complement human judgment, allowing security teams to make informed decisions and tackle more complex tasks that require in-depth knowledge.

As AI becomes more integrated into cybersecurity, ethical and legal considerations will grow in importance. Clear regulations and frameworks for responsible AI use will ensure these tools enhance security without compromising privacy or violating legal boundaries.

In summary, AI has the potential to revolutionize penetration testing and cybersecurity. By improving models, integrating threat intelligence, and ensuring responsible use, AI can help security teams stay ahead of evolving threats.

VII. ETHICAL AND LEGAL CONSIDERATIONS IN USING AI FOR PENETRATION TESTING

As AI becomes more involved in penetration testing, it raises important ethical and legal concerns. Privacy is a major issue, as AI systems can inadvertently access or expose sensitive data during testing. Given the confidential nature of many systems tested, any breach could have serious consequences, including legal repercussions.

Accountability is another challenge. With AI handling tasks traditionally performed by human testers, it becomes unclear who is responsible for mistakes – whether it's the AI, its developers, or the security team. This creates ambiguity in determining liability, especially if AI causes unintended harm, such as disrupting operations or exploiting vulnerabilities incorrectly.

Legal compliance is also critical. Penetration tests are subject to regulations, requiring explicit consent from the organization being tested. AI tools could potentially overstep these boundaries, violating laws on unauthorized access. It's essential that AI tools are built to operate strictly within the legal framework and permissions granted.

Transparency in AI decision-making is also a concern. Many AI tools work as "black boxes", making it difficult to understand their reasoning. This lack of clarity can undermine trust, especially if the AI flags vulnerabilities that are hard to explain or justify. AI tools must be designed to provide clear, understandable outputs to ensure security teams can verify their findings.

Finally, the potential for AI misuse is a serious ethical issue. While AI can defend against cyber threats, it could also be weaponized by malicious actors to automate attacks. Developers, organizations, and governments must ensure AI is used responsibly for security purposes and not for malicious activities.

In conclusion, AI in penetration testing offers great potential but requires careful consideration of privacy, accountability, compliance, transparency, and misuse. Establishing strong ethical guidelines and legal frameworks is crucial to ensure AI enhances security without compromising integrity.

VIII. CONCLUSION

This study examined how artificial intelligence is changing penetration testing and improving cybersecurity methods. Artificial intelligence tools greatly enhance the detection of vulnerabilities, boosting both precision and efficiency. Utilizing machine learning, these tools can analyze extensive datasets and detect vulnerabilities that conventional methods may miss.

Nonetheless, the article also emphasized persistent challenges, including keeping artificial intelligence current with new threats and comprehending how these systems arrive at decisions. Although artificial intelligence can handle numerous tasks automatically, human knowledge is crucial for understanding outcomes and tackling new or unexpected problems. Going ahead, an integration of artificial intelligence's capabilities and human insights is expected to be the most efficient strategy for cybersecurity.

References

[1] McKinnel, D. R., Dargahi, T., Dehghantanha, A., & Choo, K. K. R. (2019). A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. *Computers & Electrical Engineering*, *75*, 175–188. DOI: https://doi.org/10.1016/j.compeleceng.2019.02.022.

[2] Stefinko, Y., Piskozub, A., & Banakh, R. (2016, February). Manual and automated penetration testing. Benefits and drawbacks. Modern tendency. In *2016 13th international conference on modern problems of radio engineering, telecommunications and computer science (TCSET)* (pp. 488–491). IEEE. DOI: https://doi.org/10.1109/TCSET.2016.7452095.

[3] Getting PWN'd by AI: Penetration testing with large language models. In *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (pp. 2082–2086). DOI: https://doi.org/10.48550/arXiv.2308.00121.

[4] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419. DOI:https://doi.org/10.1016/j.jisa.2019.102419.

[5] Alhamed, M., & Rahman, M. H. (2023). A systematic literature review on penetration testing in networks: future research directions. *Applied Sciences*, *13*(12), 6986. DOI: https://doi.org/10.3390/app13126986.

[6] Tlachenska, E., Ivanov, K., Nenova, M., Valkova-Jarvis, Z., & Kassev, K. (2024, June). Approaches for Implementing Artificial Intelligence in Cyber-security to Improve, Speed up and Optimize Processes. In *2024 Ninth Junior Conference on Lighting (Lighting)* (pp. 1–3). IEEE. DOI: https://doi.org/10.1109/Lighting62260.2024.10590694.

[7] Li, Z., Zou, D., Tang, J., Zhang, Z., Sun, M., & Jin, H. (2019). A comparative study of deep learning-based vulnerability detection system. *IEEE Access*, *7*, 103184–103197. DOI: https://doi.org/10.1109/ACCESS.2019.2930578.

[8] Jaber, A., & Fritsch, L. (2022, October). Towards ai-powered cybersecurity attack modeling with simulation tools: Review of attack simulators. In *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing* (pp. 249–257). Cham: Springer International Publishing. DOI: https://doi.org/10.1007/978-3-031-19945-5_25.

[9] Abdirahman, A. A., Hashi, A. O., Romo Rodriguez, O. E., & Elmi, M. A. (2024). Prediction of vulnerability severity

using vulnerability description with natural language processing and deep learning. International Journal of Electrical & Computer Engineering (2088–8708), 14(4). DOI: http://doi.org/10.11591/ijece.v14i4.pp4551-4562.

[10] Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEe Access*, *10*, 93104–93139. DOI: https://doi.org/10.1109/ACCESS.2022.3204051.

[11] George, A. S. (2024). Emerging Trends in AI-Driven Cybersecurity: An In-Depth Analysis. *Partners Universal Innovative Research Publication*, *2*(4), 15–28. DOI: https://doi.org/10.5281/zenodo.13333202.

[12] Saadallah, M., Shahim, A., & Khapova, S. (2025). Optimizing AI and Human Expertise Integration in Cybersecurity: Enhancing Operational Efficiency and Collaborative Decision-Making. DOI: https://doi.org/10.56831/PSEN-06-177.

[13] Badarneh, H. J., Attiany, L. A., Asassfeh, M., Al-Shaikh, A. A., Afaneh, S., Shquier, M. M. A., ... & Samara, G. (2024, December). The power of Network Penetration Testing. In *2024 25th International Arab Conference on Information Technology (ACIT)* (pp. 1–6). IEEE. https://doi.org/10.1109/ACIT62805.2024.10877214

[14] Weerabangs, N. (2022, December 11). Intruder online vulnerability scanner review. Bug Zero. Available at: https://blog.bugzero.io/intruder-online-vulnerability-scanner-review-aea523c1e7af.

[15] Acunetix (n. d.). Introduction to Acunetix. Available at: https://www.acunetix.com/support/docs/introduction/

[16] Piconese, F., Hakkala, A., Virtanen, S., & Crispo, B. (2020). Deployment of Next Generation Intrusion Detection Systems against Internal Threats in a Medium-sized Enterprise. *Masters Thesis*. Available at: https://core.ac.uk/download/347181142.pdf.

[17] Mezquida Salva, C. (2019). Desplegar la herramienta "Bro IDS" y su posterior explotación para el análisis de actividades sospechosas en la red. Available at: https://openaccess.uoc.edu/handle/10609/107627.

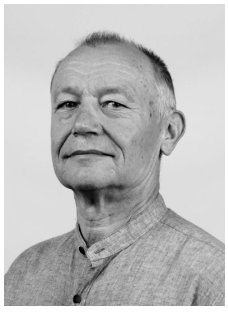
[18] Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of deep learning to real-time Web intrusion detection. *Ieee Access*, *8*, 70245–70261. DOI: https://doi.org/10.1109/ACCESS.2020.2986882.

[19] Palmgren, K., & Nordstrand, S. (2022). Metodologisk jämförelse av automatiserade och manuella penetrationstestning: En studie på bristen av manuella penetrationstestare. Available at: https://www.diva-portal.org/smash/get/diva2:1678650/FULLTEXT01.pdf.

[20] Razak, A. A., Ruzaili, H. H. H., & Zolkipli, M. F. (2024). Study on Machine Learning Implementation in Cyber-security for Security Defend and Attack. *Borneo International Journal eISSN 2636-9826*, *7*(2), 27–40. Available at: https://majmuah.com/journal/index.php/bij/article/view/635.

[21] Chakrabarty, B., Patil, S. R., Shingornikar, S., Kothekar, A., Mujumdar, P., Raut, S., & Ukirde, D. (2021). *Securing Data on Threat Detection by Using IBM Spectrum Scale and IBM QRadar: An Enhanced Cyber Resiliency Solution*. IBM Redbooks. Available at: https://books.google.com.ua/ books?id=c69CEAAAQBAJ&pg=PA8

Mariia Kozlovska is a senior in the Cybersecurity program with a specialization in Security Systems Administration at Lviv Polytechnic National University. She is focused on cybersecurity research, particularly penetration testing, vulnerability assessment, and AI-driven solutions for enhancing system security.



Volodymyr Khoma is a professor at the Institute of Control Engineering, Opole University of Technology, Poland. His research focuses on applying artificial intelligence in cybersecurity, securing embedded systems, and developing advanced methods and algorithms for digital signal processing.

Andrian Piskozub is an associate professor at the Department of Information Protection at Lviv Polytechnic National University. He is focused on cybersecurity research, computer networks security, penetration testing, and vulnerability assessment