IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, March 2026
Impact Factor: 8.2

Review of AI-Assisted and Automated Penetration Testing Techniques

Aditya Agale, Arpit Kadam, Vedangee Poyeraker, Dr. Renuka Deshpande
Dept. of Artificial Intelligence & Machine Learning
Shivajirao S. Jondhale College of Engineering, Dombivli (E), India

Abstract: *This review surveys recent advances in automated and AI-assisted penetration testing, focusing on the design and evolution of intelligent security assessment frameworks. We examine the transition from traditional manual and tool-driven penetration testing approaches toward automated systems enhanced by machine learning and large language models (LLMs). The paper analyzes how modern AI-based techniques integrate reconnaissance tools, vulnerability scanners, and reasoning models to improve contextual understanding and decision-making during security assessments. A critical review of existing automated and LLM-assisted penetration testing frameworks is presented, comparing their capabilities, limitations, and practical applicability in enterprise environments. The review further discusses challenges related to false positives, scalability, explainability, and ethical considerations in AI-driven security testing. By synthesizing state-of-the-art literature and identifying key research gaps, this review aims to provide researchers and practitioners with a clear understanding of current trends, limitations, and future directions in intelligent penetration testing.*

Keywords: *Artificial intelligence*

DOI: 10.48175/IJARSCT-31870