ID 87

A Review of Machine Learning Driven Automated Ethical Hacking: Proactive Defense and Vulnerability Mitigation in Wi-Fi and LAN Networks

TYW Bandara[1#] and DVDS Abeysinghe[2]

[1,2]Department of Computer Science, Faculty of Computing, General Sir John Kotelawala Defence University

[#]39-bse-0012@kdu.ac.lk

Abstract

The increasing reliance on Wi-Fi networks has raised significant concerns over network security, with vulnerabilities such as de-authentication, man-in-the-middle (MITM), and denial-of-service (DoS) attacks persisting despite advancements like WPA2. Tools like Aircrack-ng and Wireshark require significant technical expertise and primarily focus on vulnerability identification without offering automated feedback or proactive defenses, limiting their accessibility. This study addresses these limitations by integrating machine learning algorithms, including anomaly detection and classification models, into penetration testing. Machine learning enables the automation of vulnerability assessments, real-time threat detection, and delivery of actionable security recommendations. By analyzing network patterns and identifying irregularities, these algorithms can predict potential threats and proactively mitigate risks. Survey findings reveal a strong user preference for automated tools with intuitive guidance and proactive features like automatic hacker blocking. Based on these insights, the proposed ML-driven ethical hacking tool simplifies network security for both technical and non-technical users. The tool leverages ML to not only detect vulnerabilities but also provide dynamic remediation strategies, bridging the gap between technical complexity and usability. Result of this review emphasizes the transformative potential of machine learning in modern network security by automating processes, enhancing accessibility, and improving proactive defenses for Wi-Fi and LAN networks. By addressing key gaps in current penetration testing approaches, this research contributes to the development of innovative and efficient solutions for mitigating network vulnerabilities in an increasingly connected world.

Keywords: *Wi-Fi security, Machine learning, Ethical hacking, Automated vulnerability assessment, Proactive defense*