ID 44

Unveiling Hidden Threats: A Comprehensive Review of Host-Based Intrusion Detection, Risk Dynamics, and Proactive Defense

DAMS Priyakantha[1#], RPS Kathriarachchi[2], and SMDN Siriwardana[3]

[1,2]Department of Information Technology, Faculty of Computing, General Sir John Kotelawala Defence University
[3]Department of Computer System Engineering, Faculty of Computing, Sri Lanka Institute of Information Technology, Malabe,Sri Lanka

[#]39-bit-0018@kdu.ac.lk

Abstract

Advancements in Information Technology have given rise to an increasingly interconnected global landscape, simultaneously elevating the criticality of cybersecurity due to the growing sophistication of cyber threats. Exploiting vulnerabilities within systems and networks, cybercriminals pose significant risks to confidentiality, integrity, and availability cornerstones of modern digital infrastructure. Among the various defense mechanisms, Host-Based Intrusion Detection Systems (HIDS) have emerged as pivotal tools for detecting and mitigating these evolving threats. Nevertheless, traditional signature-based detection approaches remain inadequate in addressing contemporary challenges, including zero-day exploits, ransomware, and Distributed Denial of Service (DDoS) attacks. This study conducts a systematic review of recent advancements in HIDS technologies, emphasizing the integration of Machine Learning and Artificial Intelligence (AI) for anomaly detection and predictive analytics to enable real-time threat responses. Utilizing PRISMA guidelines, the research synthesizes findings from the literature to identify key limitations and propose enhancements to HIDS performance. The analysis reveals that AI-driven models, such as ensemble learning techniques and adaptive algorithms, significantly enhance detection accuracy, reduce false positive rates, and improve incident response times. Furthermore, the review underscores the importance of integrating HIDS with Next-Generation Firewalls (NGFW) to create a multi-tiered defense framework. NGFWs effectively filter known threats, while HIDS specialize in identifying complex and sophisticated attack patterns, thereby fostering resilience against dynamic cyber threats. This paper also outlines future research directions, including advanced AI integration, cross-network intelligence sharing, and proactive risk management frameworks, to enhance HIDS capabilities and adapt to the continuously evolving cyber threat landscape.

Keywords: *Risk dynamics, Cybersecurity, Host-based intrusion detection system, Anomaly detection, Artificial intelligence*