National Conference on Latest Innovations in Engineering, Science, Management and Humanities (NCLIESMH – 2024)

26th May, 2024, Raipur, Chhattisgarh, India.

CERTIFICATE NO : NCLIESMH /2024/C0524584

A Study of Advancing A Complete System for Anomaly Based NIDPS

Dogiparthy Sravankumar

Research Scholar, Department of Computer Science, Mansarovar Global University,
Sehore M.P., India.

ABSTRACT

An Anomaly-Based Network Intrusion Detection and Prevention System (NIDPS) is an important security mechanism used to detect and prevent unusual or malicious activities within a computer network. The advancement of a complete anomaly-based NIDPS focuses on improving the ability of the system to identify unknown attacks and abnormal network behaviors that traditional signature-based systems may fail to detect. In such systems, normal network traffic patterns are first analyzed and modeled using statistical techniques, machine learning algorithms, or artificial intelligence methods. Once a baseline of normal behavior is established, the system continuously monitors network activities and compares them with the established model. Any deviation from the normal pattern is considered an anomaly and may indicate a potential security threat such as malware, unauthorized access, or distributed denial-of-service (DDoS) attacks. Advancing a complete anomaly-based NIDPS also involves enhancing accuracy, reducing false positives, and improving real-time response mechanisms. Modern approaches integrate deep learning, data mining, and adaptive learning techniques to make the system more intelligent and efficient. Furthermore, scalability, faster processing of large network data, and integration with existing security infrastructures are essential components of an advanced NIDPS. Therefore, developing a comprehensive anomaly-based NIDPS plays a significant role in strengthening cybersecurity and protecting organizational networks from emerging and sophisticated cyber threats.