Design of a network attack detection and monitoring system using IDS/IPS and ELK Stack.

Bui Ngoc Chinh

Abstract: In the context of increasingly severe cybersecurity threats, this study aims to design and implement a network attack detection and monitoring system based on IDS/IPS and the ELK Stack. Addressing common security threats in real-world network environments, this project ensures data security and integrity by integrating Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Additionally, leveraging the log management tool ELK Stack for real-time analysis further enhances system performance and response speed. Combining theoretical analysis with practical application, the research aims to provide users with a comprehensive and efficient network security solution. This system not only effectively identifies potential threats but also optimizes defense strategies through data analysis, thereby strengthening overall network security.

Keywords: Cybersecurity, IDS/IPS, ELK Stack