Building a network monitoring and attack detection system based on the open-source ELK Stack

Nguyen Hoang Duong

Abstract: In the context of the increasing number of cyber attacks, this topic focuses on building a network monitoring and attack detection system using the open-source ELK Stack. The goal is to create an effective solution to protect important information in the network environment. The research method combines theory with experimentation, including the deployment and optimization of ELK Stack components. The expected results of this topic will not only raise awareness about cybersecurity but also contribute to the community by providing an open-source system that can be widely used.

Keywords: Monitoring system, cyber attack, ELK Stack, information security, open source