Research and build an intrusion prevention and detection system using Snort/SnortSam.

Nguyen Dang Son

Abstract: In the context of increasingly developing information technology, network security has become more important than ever. This topic focuses on researching and building an intrusion prevention and detection system using Snort/Snortsam as an effective solution. The objective of the study is to explore Snort's policy rules to build a system for monitoring network traffic and early detection of any intrusion activities. The research methodology includes both theoretical analysis and practical application deployment, aiming to enhance security effectiveness for organizations. The significance of this topic lies in providing knowledge and practical tools about Snort/Snortsam, thereby contributing to the field of network protection.

Keywords: Snort, Snortsam, intrusion detection system, network security, policy rules