Building a Honeypot system to collect and analyze cyber attack behavior

Lai Tuan Dat

Abstract: In the context of increasingly severe cybersecurity issues, this study aims to design and implement a Honeypot system to collect and analyze network attack behaviors. Based on a combination of theoretical and empirical methods, a virtual environment capable of simulating real services is constructed, and malicious access activities from external sources are monitored in real time. Through the application of this system, different types of attack methods and their sources can be effectively identified and classified, thereby providing data support and decision-making basis for cybersecurity strategies. This study not only fills a gap in data analysis methods in certain specific security domains but also lays a solid foundation for more in-depth future research.

Keywords: Honeypot, network security, attack behavior analysis, virtual environment, data-driven