Building and experimenting with a network forensics analysis process in a virtualized environment.

Ngo Thi Hai Yen

Abstract: In the context of network security analysis, research and application in virtualized environments are crucial for ensuring the security of network systems. This thesis aims to address the challenges of network intrusion forensic analysis by developing a network intrusion analysis process suitable for virtualized environments through a combination of theoretical research and experimental validation. Utilizing advanced data collection techniques, real-time monitoring, and log analysis methods, this paper not only constructs an efficient and reliable network intrusion detection framework but also demonstrates the effectiveness of the proposed solution through practical cases. The significance of this work lies in filling the gap in the application of existing network security solutions in virtualized environments, providing strong support for improving network security.

Keywords: Cybersecurity, network forensic analysis, virtualized environment, intrusion detection, data collection