ABSTRACT

This research aims to analyze network security in web environments during Distributed Denial of Service (DDoS) attacks using the Live Forensics method. DDoS attacks pose a serious threat to organizations and companies that rely on information technology. The Live Forensics method is employed for real-time analysis of DDoS attacks, involving the identification of attack signs, collection of relevant data, and analysis of the data to determine the source of the attacks.

The research has three main objectives. Firstly, to identify the signs of DDoS attacks occurring in web networks using the Live Forensics method. Secondly, to gather the necessary data for network security analysis during DDoS attacks using the Live Forensics method. And thirdly, to analyze the acquired data to identify the sources of DDoS attacks and determine the types of attacks.

The research methodology encompasses the formulation of the final project proposal, literature review to comprehend the employed methods, implementation of the Live Forensics method for identifying the sources of DDoS attacks, evaluation of the effectiveness of the applied methods, and compilation of a book documenting the research findings.

By applying the Live Forensics method in the analysis of network security during DDoS attacks in web environments, this research aims to assist organizations and companies in safeguarding their networks, protecting their infrastructures, mitigating business disruptions, and ensuring the security of client data and information. The insights gained from this research provide guidance for effective approaches in combating DDoS attacks and can serve as a foundation for the development of enhanced security measures against similar attacks in the future.

Keywords:

Network security analysis, Web, DDoS attacks, Live Forensics method, Identification of attack signs, Infrastructure security, Data and information security.