ABSTRACT

Network security system has a lot of variety according to the circumstances and conditions concerned. A network security system is a very important role in maintaining network security to prevent attacks and protect us in the event of an attack. Frequent attacks on a device through a network both in terms of malware administration, and data theft.

This final project focuses on the extent to which HIDS-based IDS can detect attacks that are common in the network. With the help of Honeypot Dionaea which serves as an attracter for attackers, as well as what information will be obtained when performing analysis malware using Cuckoo Sandbox. This implementation is carried out with six active users who are in one network and pay attention to whether the attacker can be detected by IDS or not.

Results from this final project found that HIDS-based IDS has the advantage of monitoring digital data and based on the results of brute force attack attempts obtained 65.55% detected an attempt to log in using an unregistered username, 29.16% detected a failed login attempt, 4.17% detected double log in short time, and 1.11% detected a bruteforce attempt to gain access to the system. Cuckoo Sandbox can provide malware information in the form of what types of malware are analyzed, how the malware behaves, and how it impacts the malware on the systems attacked.

Keywords: *Honeypot, IDS, Malware, Malware Analysis System*