ABSTRACT

IMPLEMENTATION OF HONEYPY WITH MALICIOUS TRAFFIC DETECTION SYSTEM (MALTRAIL) USING DESCRIPTION ANALYSIS TO DETECT DOS ATTACKS ON SERVERS

By

Halim Alfidzar

18102195

In today's era, there are still many attacks on servers that make the server will experience damage to the operating system. Examples that are often found are DoS attacks. In prevention, security or reference is needed to support security for the server. Network and server security is very important because many attacks have been carried out by irresponsible parties. We need a treatment that can analyze attacks against several threats. HoneyPy with Maltrail is an open-source application that can be used for proof methods in research. There is CentOs which is used as an additional server and Linux Mint as the main server. The attacks carried out in this study were carried out by the researchers themselves on the server using DoS attacks. The data collected from maltrail will be analyzed using descriptive analysis, the results of this study are HoneyPy with Maltrail being able to be a benchmark to be used as an increase in security on attacks on the server. Based on the test, it was found that the results were five reports that obtained three threats, six events, detected low and medium severity, one threat source at the source, and four traces.

Keywords: Security, Server, Maltrail, HoneyPy, DoS.