ABSTRACT

Today's internet technology is not free from many problems or security holes. This security hole could be exploited by an unauthorized person to steal important data. The case of the attacks occurred because the party that was attacked also did not realize the importance of network security to be applied to the system.

Honeypot is a system that is designed to resemble the original production system and is made with the intention to be attacked / compromised. Honeypot implemented using low interaction honeypot Glastopf as well as using other supporting software. Durability test conducted with direct attacks to determine the safety of the system.

The results of this research is low interaction honeypot on embedded system with the form of Cubieboard that can emulate vulnerabilities such as directory buster brute force, LFI, and RFI. One of the results of stress tests with 773 samples, obtained average time of 5275 ms, 2067 ms deviation, throughput 367.012 samples per minute, and with median 5831 ms conducted with 50 threads and 10 ramp-ups per second.

Keywords: honeypot, Cubieboard, low interaction, web server, security.