ABSTRACT

The use of information technology will be applied in all areas of daily life has become something that is familiar today. Of all ages can easily access the Internet. One of the tools that we can rely on as a virtual security system is a honeypot. With honeypot system will 'cheat' or giving false data if there are people who have bad intentions when he entered into an information system.

In this final project implementation Honeyd honeypot in place on the main server, which functions as a 'net' to fool the intruder attacks. On the main server will be created the File Transfer Protocol, FTP services how strong survive if there is an attack from intruders. In this case the intruder in the form of wear testers attacks Denial of Services (DoS) so that administrators will determine performance comparison when no attack, when there is an attack, and when deflected into the fake port run by Honeyd and Snort IDS. Before the experiment we used to test the resilience of the FTP server with the ping flooding attack to determine the threshold at IDS Snort rules. In order for such a network of real network traffic generated by 5 Mbps. Then analysis of performance, in 3 trials with different conditions. On the server side performance is seen that history CPU, RAM usage, bitrate data, and processing time. As a result of the attacks of DoS, CPU history reached 94.7% and the system will be down if it reaches 100%. Once there Honeyd, CPU history had dropped to below 85%, so that the FTP service will return to normal. Honeyd the response time needed to restore normal conditions about 20 to 25 seconds.

Keywords ***: HoneyD, Snort IDS, File Transfer Protocol, Ping Flooding Attack, Iperf, Performance***