ABSTRACT

Technology nowadays is growing rapidly, both from its complexity and its size. Based on the statistical result, the level of computer network's exploitation has been increased day by day. It correspondingly goes with the increase of knowledge, technique, and tools that is used to do the attacks. Actually, the defense system technologies of attack are already existed, but the development has exceeded the limit so it is no longer efficient because it cannot guarantee the accuracy of security. One of those techniques is *Intrusion Detection Systems* (IDS), but the weakness is sometimes it is unable to detect the invalid packet because of the high-traffic. Then Honeypot becomes the one to overcome this problem.

This final project describes about the design and implementation of Honeypot security system on VoIP services--on which is today, the attack keeps increasing, such as the attack of DoS (*Denial of Service)*. Besides, the attack pattern then can be used as the reference to mend the existing defense system, like firewall and IDS.

From the result, Honeypot Artemisa has successfully implemented into VoIP domain, proven by the successful fake server and VoIP client that tricks the attacker to penetrate into the Honeypot system.. Through this way, the attacker's information like ip address, port, tools, etc can be identified as well so it would be beneficial for the server's network security. When a DoS attack the honeypot cpu load value will increase from 6.2% to 65%. Similarly, the VoIP server which rose significantly from 19.7 to 98.1%. This becomes very risky because it reduces system availability so, the use of firewall can protect the server more from availability and access control attacks for a the server where the event of a DoS attack cpu load is only increased to 56.8% when compared to the server without a firewall at an interval of 3 minutes.

Key word : honeypot, IDS, *Firewall*, VoIP