ABSTRACT

Network security system in fact is very much its kind in accordance with the circumstances and conditions in question. And almost entirely just talking about protecting and dispel the attack in the absence of more value that can be utilized. So we can only protect our system can analyze it without further. For it needs to make a system that can make an attack able to deliver value for the benefit for us.

This final project evaluates the performance of security system as a trap and threat detection. The excellence of *honeypot dionaea* is it's ability of gaining the copy of malware sent by the attacker. Thus, the administrator can take further action like analyzing the malware using *Malware Analisys Toolkit*.

From the testing result, *Dionaea* is seen as a trap which is able to capture the malware and put it into binaries folder. The test is done in public network during 14 days with eleven malwares captured. The service that is mostly attacked is Mssql, while the least is HTTP. Both forover public and private network, the attack detector can detect the real time threats steadily—but false negative and positive still exist. And *Cuckoo Sandbox* as a *Malware Analisys Toolkit* can gather the malware information which is useful for future research.

Keyword : *Honeypot, Dionaea, IDS, Malware, Malware Analisys Toolkit, Cuckoo Sandbox*