Abstract

Information is a very important commodity. The importance of an information value makes the information becomes very important to be protected especially sensitive information. To achieve this objective some security and prevention efforts are developed in order to make security system more reliable in protecting information. One of the security efforts that can be done is by implementing infiltration prevention techniques.

Intrusion Prevention System (IPS) is intrusion prevention software that combines two functions, namely firewalls functions and intrusion detection system (IDS). With the combination of these two functions, IPS is capable on performing detection and protection functions that can be done simultaneously and automatically. To perform detection, IPS is built by using a snort IDS. Snort IDS is a security system based on open source that can be implemented in a multiplatform network. As for the blocking function, it uses the IPTables firewall. The workings of the IPS is by reading the IP header of the attacker and by matching with rules that have been defined, then command a firewall to block the IP address when it has appeared alert, indicating the system finds a suspicious IP address.

Therefore, final project, which entitled "Implementation of Intrusion Prevention System (IPS) Using Web Based Snort IDS and IPTables Firewall", is one way to overcome it. Web IPS is a system IPS that be connected to dashboard web then web uses as a web interface which is used to run (start / stop) configuration of the system, while displaying the data alert report and intrusion which is generated by the IPS server.

Keywords : Intrusion Prevention System, Alert, Intrusion, block, web IPS