ABSTRACT

Today, internet users are increasingly increasing. But it actually has an impact on the increasing types of interference on the Internet that harm users who use the Internet network. Attacks launched by the attacker against the target (internet users) vary. For example Distributed Denial of Service (DDOS) attacks, Brute Force and Scanning.

System Administrator (Sysadmin) is responsible for managing and maintaining the server for specific needs. But the server can be attacked at any time by irresponsible parties. In order to facilitate sysadmins to know what attacks occur on the server, then the need for attack detection.

In this final project, analysis of Distributed Denial of Service, Brute Force and Scanning attacks has been performed and the output of the analysis is a rules for attack detection by using decision tree algorithm. Based on the capabilities of the Decision Tree Algorithm in performing attack detection, each attack has been detected. Accuracy of Distributed Denial of Service, Brute Force, and scanning attacks 30 times on average is 99.35%, ssh brute force 94.57% and scanning 98.11%.

Keywords : *Decision Tree, DDoS, Brute Force, Scanning, Sysadmin.*