The 2nd Conference on Management, Business, Innovation, Education, and Social Science (CoMBInES)

Taichung, Taiwan 3-6 March, 2022

IMPROVING WIRELESS NETWORK SECURITY BY APPLYING SECURITY POLICY TO FIREWALL

Muhammad Jufri, Heryanto
Faculty of Computer Science, University Internasional Batam
{jufri@uib.edu 1831150 .heryanto@uib.edu}

ABSTRACT

Current technological developments have a significant impact on human performance in fulfilling daily activities. The development of technology makes crime in the network more widespread so that network security is very influential on the prevention of attacks carried out by attackers. Examples of crimes such as theft of company data that cause harm to the company as well as other crimes. For that, a system that can detect attacks such as Denial of Service, Ping Attack, and Port Scanning. Intrusion Detection System (IDS) serves to monitor every network traffic that passes. The purpose of the study is to define the security of wireless networks and get results from the use of IDS. This implementation is carried out on the Linux Ubuntu operating system version 18.04 LTS using snort and Iptables as an attack deterrent. After that, use the opensource wireshark tool as an analysis of attacks that occur in the network. The research method used is the Security Policy Development Life Cycle (SPDLC) by passing through several stages, namely: Analysis, Design, Implementation, Enforcement, Enchancement. The results concluded that attacks carried out by attackers on the network can be known and handled before wider damage occurs as well as the use of wireshark that can analyze attacks properly through the flow graph provided.

Keywords: *Linux, Iptables, Network Security, Security Policy Development Life Cycle (SPDLC), Intrusion Detection System (IDS)*