ABSTRACT

IMPLEMENTATION OF PORT KNOCKING ON MIKROTIK BY APPLYING INTRUSION PREVENTION SYSTEM (IPS) FOR NETWORK SECURITY SYSTEMS

By

Muhammad Nur Fauzi Akmal Akbar

18102133

In today's era of modern technology, computer network security is a very important thing to pay attention to. A computer network is a system consisting of several computers designed to be able to share data, information and resources. The increasing number of intrusions or attacks carried out by hackers is one of the main factors in this case, especially when the server computer is connected to the Internet, attacks will increase and various attack techniques continue to develop including Port Scanning and DDoS which cannot be ignored. Based on the problems that occur, the authors need to monitor network access and prevent unauthorized use of network resources by using the Port Knocking method from Mikrotik and the Intrusion Prevention System (IPS) on servers that can withstand cyber attacks in the form of Port Scanning and DDoS. Mikrotik is a computer network device in the form of hardware and software that can function as a router, as a filtering, switching and other tool. Port Knocking is the concept of hiding a remote service inside a firewall that allows access to that port only to find out the service after the client has successfully authenticated to the firewall. Intrusion Prevention System (IPS) is a device that works for monitoring network traffic, detecting suspicious activity and making early prevention of intrusions or events that can make the network run inappropriately. In the process of this method, install tools and apply Port Knocking and IPS rules on network security systems. The results of this study are the authors successfully apply Snort rules to detect and prevent DDoS attacks and successfully apply Port Knocking rules to close all ports attacked by Port Scanning, so that when an attack occurs, action can be taken quickly.

Keyword : Security Network, Intrusion Prevention System, Port Knocking, Denial of Service, Port Scanning.