DESIGN OF AN INTRUSION DETECTION SYSTEM ON SERVERS AGAINST BRUTE FORCE AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

Name : Syahrudi Amril

Id Number : 6103211455

Supervisor : Eko Prayitno, M. Kom

ABSTRACT

The intrusion detection system aims to monitor server network traffic using the Python library Scapy. The system continuously monitors both incoming and outgoing network traffic from the server and identifies suspicious activities such as Distributed Denial of Service (DDoS) and Brute Force attacks. The IDS is capable of detecting UDP Flood, TCP SYN Flood, and ICMP Flood attacks, as well as Brute Force attacks on SSH services. When a network packet is detected as an attack, the IDS displays a message containing information about the attack. This attack message is logged and sent to Telegram via a Telegram Bot for notification purposes. Testing results show that while attacks can still enter the server and affect memory and CPU usage, the implementation of the intrusion detection system allows for early detection and notification of attacks, facilitating easier response actions by administrators to minimize the impact of the attacks.

Keywords*: Intrusion Detection System, Server, Python, Brute Force, Distributed Denial of Service*