ABSTRAK

Keamanan jaringan merupakan aspek terpenting sebuah sistem dalam menjaga validitas dan integritas data, serta menjamin ketersediaan layanan bagi penggunaannya. Sistem jaringan komputer dirancang dengan tujuan dapat berbagi sumber daya untuk dipakai secara bersama, sehingga keamanan sumber daya pada server harus dijaga keamanan dan mengoptimalkan sumber daya yang digunakan. Tujuan penelitian ini adalah analisis perbandingan tingkat optimalisasi Port knocking dan Honeypot menggunakan metode IPTables untuk keamanan jaringan pada server dengan sumber daya CPU dan Memori yang lebih rendah dan lebih tinggi. Metode yang digunakan dalam penelitian ini adalah Port knocking, Honeypot dan IPTables. Metode ini memiliki lima tahapan yaitu detection, analisis, reporting, execution, dan increased security. Data yang digunakan dalam penelitian ini adalah data port yang berhasil diserang dan data penggunaan sumber daya sebelum dan setelah penerapan IPTables pada server dengan sumber daya server 2 CPUs dan 1507284KiB memori yang diperoleh dari penelitian terdahulu. Hasil dalam penelitian ini yaitu 80% dari port yang ada yaitu port 21, 53, 80 dan 2222 tidak bisa diserang dan 20% dari port yang ada yaitu port 22 dirancang agar dapat diserang karena merupakan port dari server bayangan Honeypot. Grafik penggunaan sumber daya CPU dan Memori server mengalami penurunan penggunaan setelah penambahan IPTables dari pengujian serangan Denial of Service (DoS) dan Brute force, pada server dengan sumber daya 1 CPUs dan 1015852KiB memori penggunaan CPU menurun sebesar 36% dan penggunaan memori juga menurun sebesar 41% sedangkan pada server dengan sumber daya 4 CPUs dan 6036624 KiB memori penggunaan CPU menurun sebesar 41% dan penggunaan memori juga menurun sebesar 46%pada server dibandingkan dengan hanya menggunakan metode Port knocking dan Honeypot saja. penelitian ini dapat menjadi acuan dalam mengukur optimalisasi server dalam mengatasi serangan Denial of Service (DoS) dan Brute force.

Kata Kunci: ***Port Knocking, Honeypot, IPTables, Denial of Service, Brute force.***

ABSTRACT

Network security is the most important aspect of a system in maintaining the validity and integrity of data, as well as ensuring the availability of services for its use. Computer network systems are designed with the aim of sharing resources for joint use, so that the security of resources on the server must be maintained and the resources used must be optimized. The aim of this research is a comparative analysis of the level of optimization of Port knocking and Honeypot using the IPTables method for network security on servers with lower and higher CPU and memory resources. The methods used in this research are Port knocking, Honeypot and IPTables. This method has five stages, namely detection, analysis, reporting, execution, and increased security. The data used in this research is port data that was successfully attacked and resource usage data before and after implementing IPTables on a server with server resources of 2 CPUs and 1507284KiB of memory obtained from previous research. The results of this research are that 80% of the existing ports, namely ports 21, 53, 80 and 2222, cannot be attacked and 20% of the existing ports, namely port 22, are designed to be able to be attacked because they are ports from the Honeypot shadow server. The server CPU and memory resource usage graph experienced a decrease in usage after adding IPTables from Denial of Service (DoS) and Brute force attack testing, on a server with 1 CPUs and 1015852KiB of memory CPU usage decreased by 36% and memory usage also decreased by 41%, while on a server with 4 CPUs and 6036624 KiB of memory CPU usage decreased by 41% and memory usage also decreased by 46% on the server compared to using just the Port knocking and Honeypot methods. This research can be a reference in measuring server optimization in overcoming Denial of Service (DoS) and Brute force attacks.

Keywords: Port Knocking, Honeypot, IPTables, Denial of Service, Brute force.