INTISARI

OTOMATISASI *FIREWALL RULES* PADA ROUTER BERDASARKAN DATA SERANGAN BARU PADA *HONEYPOT* MENGGUNAKAN PYTHON

Abstrak – Pada zaman revolusi industri 4.0 seperti saat ini sangat penting untuk menjaga keamanan jaringan dari serangan dunia luar karena segala sesuatu sudah terhubung ke internet. Menurut Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) tercatat ada 88.414.296 serangan sejak 1 Januari 2020 hingga 12 April 2020. Puncak jumlah serangan terbanyak terjadi pada tanggal 12 Maret 2020 sebanyak 3.344.470 serangan. *Firewall* merupakan salah satu teknologi dalam keamanan jaringan, *firewall* akan melakukan *filtering* atau penyaringan setiap data yang akan masuk maupun keluar. Dalam proses pembuatan *firewall* diperlukan ketelitian, dikarenakan banyak konfigurasi yang harus dibuat untuk setiap *rules*. Maka dari itu, dibuat sebuah sistem yang melakukan otomatisasi dalam pembuatan *firewall*. Data yang digunakan diambil dari honeypot yang kemudian mengirimkan data penyerang menuju *database*. Untuk menguji keberhasilan pembuatan *firewall rules*, dilakukan pengujian *fuzzing* yang merupakan teknik untuk mengukur tingkat keberhasilan dari sebuah sistem dengan memberikan *input* secara acak dalam durasi waktu tertentu. Hasil yang diperoleh dari pengujian *fuzzing*, membuktikan bahwa sistem otomatisasi *firewall* dapat mengurangi kesalahan penulisan *firewall rules* pada *router*.

Kata Kunci : *firewall*, otomatisasi, Ansible, Django, Djongo

ABSTRACT

AUTOMATION OF FIREWALL RULES ON THE ROUTER BASED ON NEW ATTACKING DATA ON HONEYPOT BY USING PYTHON

Abstract - In the era of the industrial revolution 4.0, it is very important to maintain network security from attackers because everything is connected to the internet. According to Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN)*, there were 88,414,296 attacks from 1 January 2020 to 12 April 2020. The peak number of attacks occurred on 12 March 2020 with 3,344,470 attacks. Firewall is one of the technologies in network security, and it will filter every incoming or outgoing data. In the process of creating a firewall, accuracy in writing the rules is needed because there are many configurations that must be made for each rules. Therefore, this system is created that automates the creation of a firewall. The data used is taken from a database that stores honeypot attacks. To get the the success rate of a firewall, a fuzzing test was carried out which is a technique for measuring the success rate of a system by providing random input within a certain time duration. The results obtained from fuzzing testing prove that the firewall automation system can minimize the typing failure of the firewall creation.*

Keywords : firewall, *automation*, Ansible, Django, Djongo