ABSTRAK

IMPLEMENTASI SISTEM KEAMANAN JARINGAN DI PSDKU UNIVERSITAS LAMPUNG WAYKANAN MENGGUNAKAN SERVER WAZUH UNTUK DETEKSI DAN RESPON SERANGAN SIBER

Oleh

Azzah Shafiyyah

PSDKU Universitas Lampung Way Kanan membutuhkan sistem keamanan jaringan yang efektif untuk melindungi jaringan komputer server lab komputer dari serangan siber yaitu *brute force* dan *Denial of Service* (DoS) Untuk meningkatkan keamanan jaringan, diperlukan implementasi sistem keamanan jaringan dengan menggunakan *platform* wazuh sebagai server monitoring dan wazuh *agent* yang diinstal pada komputer server jaringan lab komputer PSDKU menggunakan Server Utama PSDKU. Metode pengembangan sistem keamanan yang digunakan yaitu PPDIOO (*prepare, plan, design, implement, operate, optimize*) cisco. Dalam sistem ini, semua aktivitas dari wazuh agent akan dikirimkan ke wazuh server untuk dilakukan pemantauan dan deteksi serangan siber. Kemudian dilakukan simulasi serangan *brute force* dan *Denial of Service* (DoS) terhadap wazuh *agent* yang terinstal pada server jaringan lab komputer. Respon dari serangan bruteforce yang akan dilakukan adalah dengan memblokir alamat IP penyerang menggunakan *software* fail2ban dan serangan DoS dengan Active Response Wazuh sehingga penyerang tidak dapat mengakses dan tidak dapat terhubung ke komputer server jaringan lab komputer PSDKU. Sistem keamanan jaringan tidak dapat mendeteksi serangan DoS dengan jumlah rata-rata koneksi dibawah 4000 koneksi http, dan Serangan DoS berhasil dilakukan dengan hasil yang menunjukkan bahwa Server Utama PSDKU memiliki ketahanan dalam menerima dan melayani koneksi HTTP dibawah 3.522.013 koneksi. Sehingga sistem keamanan jaringan dapat ditingkatkan dan respon terhadap serangan siber dapat dilakukan secara cepat dan efektif.

Kata kunci : *Keamanan Jaringan, Brute Force, DoS,* PSDKU, *PPDIOO*

ABSTRACT

IMPLEMENTATION OF THE NETWORK SECURITY SYSTEM AT PSDKU LAMPUNG WAYKANAN UNIVERSITY USING WAZUH SERVERS FOR CYBER ATTACK DETECTION AND RESPONSE

By

Azzah Shafiyyah

To improve network security, it is necessary to implement a network security system using the wazuh platform as a monitoring server and wazuh agent installed on the PSDKU computer network server using PSDKU Main Server. The method of development of the security system used is PPDIOO (prepare, plan, design, implement, operate, optimize) cisco. In this system, all the activities of the agent will be sent to the server for monitoring and detection of cyber attacks, then simulated brute force and Denial of Service (DoS) attacks against the agent installed on the computer lab network server. The response to a bruteforce attack is to block the attacker's IP address using file2ban software and DoS attacks with Active Response Wazuh so that the attackers can't access and connect to the computer server of the PSDKU computer's lab network. The network security system could not detect a DoS attack with an average number of connections below 4000 http connections, and the DoS Attack was successfully carried out with results showing that PSDKU's Main Server has resilience in receiving and serving HTTP connections under 3.522.013 connections. So the network security system can be improved and the response to cyber attacks can be carried out quickly and effectively.

Keywords: Network Security, Brute Force, DoS, PSDKU, PPDIOO