

Implementasi dan analisis kinerja keamanan jaringan berbasis Intrusion Detection System (IDS) terhadap serangan siber pada teknologi komputasi awan = Implementation and analysis of network security performance based on Intrusion Detection System (IDS) against cyber attacks on cloud computing technology

Airell Ramadhan Budiraharjo, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=9999920544725&lokasi=lokal>

Abstrak

Penelitian ini dilakukan untuk menganalisis keamanan jaringan khususnya pada teknologi komputasi awan dari serangan siber. Hal ini didasarkan dengan melihat era sekarang di mana teknologi komputasi awan (Cloud Computing) sedang mengalami perkembangan yang pesat. Banyak perusahaan saat ini mulai beralih dari penggunaan sumber daya secara on-premises menjadi teknologi cloud berjeniskan private cloud dengan alasan efisiensi dan kemudahan yang diberikan teknologi cloud. Namun, kemudahan akses pada teknologi private cloud ini pun justru menjadi peluang yang besar oleh para peretas untuk melakukan serangan siber, seperti Port Scanning, DoS, dan Reverse shell. Oleh karena itu, diperlukan keamanan jaringan yang baik agar teknologi cloud yang digunakan terhindar dari dampak serangan siber yang merugikan. Salah satu metode keamanan yang dapat diterapkan, yaitu dengan implementasi tools Intrusion Detection System (IDS). Intrusion Detection System (IDS) berfungsi untuk mengawasi keamanan jaringan dengan melakukan pendeteksian terhadap anomali atau serangan yang dilakukan melalui analisis lalu lintas jaringan tersebut. Berdasarkan hasil dari penelitian implementasi IDS pada server komputasi awan didapat bahwa nilai rata-rata detection rate IDS dari tiga skenario pengujian serangan siber adalah sebesar 51.19% dengan rata-rata penggunaan CPU dan memori dari server selama pengujian adalah 21.23% dan 29.20%. Hal ini menunjukkan bahwa IDS menunjukkan potensi sebagai tools yang efektif dalam meningkatkan keamanan pada platform cloud computing tanpa memberikan dampak negatif yang berarti terhadap performa perangkat.

.....This research was conducted to analyze network security, especially in cloud computing technology from cyber attacks. This is based on looking at the current era where cloud computing technology is experiencing rapid development. Many companies are now starting to switch from using on-premises resources to private cloud technology due to the efficiency and convenience that cloud technology provides. However, this ease of access to private cloud technology is also a huge opportunity for hackers to carry out cyber attacks, such as Port Scanning, DoS, and Reverse shell. Therefore, good network security is needed so that the cloud technology used can avoid the harmful effects of cyber attacks. One of the security methods that can be applied is the implementation of Intrusion Detection System (IDS) tools. This Intrusion Detection System (IDS) aims to monitor network security by detecting anomalies or attacks through analyzing network traffic. Based on the results of the IDS implementation research on the cloud computing server, it is found that the average IDS detection rate from three cyber attack test scenarios is 51.19% with the average CPU and memory usage of the server during testing is 21.23% and 29.20%. This shows that IDS shows potential as an effective tool in improving security on cloud computing platforms without having a significant negative impact on device performance.