IMPLEMENTASI IDENTIFIKASI SERANGAN *DENIAL OF SERVICE* (DOS) BERBASIS *BRUTE FORCE* MENGGUNAKAN WIRESHARK

Salsha Febrianinda[1], Muhammad Faqih Dzulqarnain[2], Irwan Adhi Prasetya[3]

INTISARI

Latar Belakang: Kejahatan siber menjadi ancaman dalam kehidupan manusia, sehingga menyulitkanm organisasi dan pemerintah untuk mengatasi kejahatan yang dilakukan dalam teknologi komputer. Kejahatan ini berdampak buruk pada masyarakat, perusahaan, perbankan, dan lainnya. Salah satu *cybercrime* yang sering terjadi pada suatu jaringan dan sistem yaitu *Denial of Service (DOS) Attack* dan *Brute force Attack*. Untuk mengurangi dan mencegah dampak serangan kejahatan *cyber* pada dunia digital, maka dibutuhkanlah *cyber security* atau kemananan siber yang bertugas untuk mencegah dan melindungi sistem komputer maupun data. Metode: *Anomaly-based:* Melakukan monitoring lalu lintas paket dan membandingkannya dengan pola lalu lintas normal sistem *(baseline)* terhadap intrusi. Jika ada lalu lintas yang mencurigakan dan tidak sesuai *baseline* maka akan diidentifikasi dan memberikan peringatan kepada administrator serta melakukan pencegahan. Karena adanya *baseline*, metode deteksi ini dapat mendeteksi serangan jenis baru yang masuk kedalam sistem. Hasil dan Kesimpulan: Implementasi penindakan serangan *Denial of Service* (DoS) berbasis *brute force* menggunakan Wireshark efektif dalam mendeteksi lalu lintas jaringan yang mencurigakan. Wireshark dapat menganalisa mendalam terhadap paket data yang melewati jaringan, sehingga serangan dapat diidentifikasi secara cepat dan akurat.

Kata Kunci **:** *Brute force*, serangan *Denial of Service*, kejahatan siber
Kepustakaan **:** 16 Jurnal (Tahun 2019-2024)
Jumlah Halaman **:** xi; 60 Halaman; Tabel 2.1 s.d Tabel 3.2; Gambar 3.1 s.d Gambar 4.19

[1.] Mahasiswa Prodi D-III Teknologi Informasi Politeknik 'Aisyiyah Pontianak

[2.] Dosen Politeknik 'Aisyiyah Pontianak

IMPLEMENTATION OF DENIAL OF SERVICE (DOS) ATTACK IDENTIFICATION BASED ON BRUTE FORCE USING WIRESHARK

Salsha Febrianinda [1], Muhammad Faqih Dzulqarnain[2], Irwan Adhi Prasetya[3]

ABSTRACT

Introduction: Cybercrime poses a significant threat to human life, making it challenging for organizations and governments to tackle crimes committed through computer technology. These crimes have adverse effects on society, businesses, banks, and other sectors. Two common types of cybercrime that often occur within networks and systems are Denial of Service (DOS) Attacks and Brute Force Attacks. To mitigate and prevent the impact of cyber attacks in the digital world, cybersecurity is essential. Cybersecurity aims to prevent and protect computer systems and data. Method: Anomaly-based Detection: This method involves monitoring packet traffic and comparing it to the system's normal traffic patterns (baseline) to detect intrusions. If suspicious traffic that deviates from the baseline is detected, it will be identified, and an alert will be sent to the administrator, along with preventive actions. Due to the presence of a baseline, this detection method can identify new types of attacks entering the system. Result and Conclusion: The implementation of mitigation measures against Denial of Service (DoS) attacks based on brute force using Wireshark is effective in detecting suspicious network traffic. Wireshark can deeply analyze the data packets passing through the network, allowing for quick and accurate identification of attacks.

Keywords **:** Brute force, Denial of Service attack, cyber crime.
Literature **:** 16 Journals (2019-2024)
Pages **:** xi; 60 Pages; Table 2.1 to Table 3.2; Picture 3.1 to Picture 4.19

[1.] Mahasiswa Prodi D-III Teknologi Informasi Politeknik 'Aisyiyah Pontianak

[2.] Dosen Politeknik 'Aisyiyah Pontianak