ABSTRAK

Penggunaan jaringan komputer secara global, seperti internet, memberikan kemudahan dalam menyelesaikan berbagai pekerjaan. Namun, kemudahan ini juga memicu adanya penyalahgunaan akses tidak sah (un-authorized access) untuk melakukan kejahatan tertentu. Untuk mencegah hal tersebut, administrator jaringan perlu menerapkan strategi guna memastikan jaringan tetap aman dari akses yang tidak berwenang. Salah satu sistem pengamanan jaringan yang umum digunakan adalah firewall, yang berfungsi melindungi data dari pengguna yang tidak memiliki hak akses. Salah satu jenis serangan yang sering terjadi seperti serangan Denial of Service (DoS) yang bertujuan menguras sumber daya komputer dengan menargetkan pada windows server di suatu instansi, sehingga pengguna lain kesulitan mengakses komputer yang diserang. Dalam menjaga integritas, kerahasiaan, dan ketersediaan data, monitoring keamanan jaringan menjadi aspek krusial. Penelitian ini mengusulkan penggunaan metode forensik jaringan untuk analisis lalu lintas jaringan dalam mendeteksi dan merespons insiden keamanan menggunakan Wireshark, untuk mendeteksi serangan Distributed Denial of Service (DDoS). Wireshark mampu menangkap paket data yang melintas di jaringan, sehingga dapat mengidentifikasi pola serangan DDoS seperti lonjakan lalu lintas yang tidak normal dan paket mencurigakan. Melalui simulasi serangan DDoS, penelitian ini menunjukkan bagaimana metode forensik jaringan dapat digunakan secara efektif untuk mendeteksi, menganalisis, dan merespons serangan siber.

Kata kunci : Network Security, Firewall, Denial of Service, Forensik Jaringan.

DAFTAR ISI