

ABSTRAK

Nama : Albilal Kahfi
NIM : 41520010008
Program Studi : Teknik Informatika
Judul Proposal Penelitian : Deteksi dan Analisis serangan DDoS menggunakan Wireshark dan Snort
Pembimbing : Prof. Dr. Ir. Rahmat Budiarto

Deteksi dan Analisis Serangan DDoS Menggunakan Wireshark dan Snort, Penelitian ini bertujuan untuk mendeteksi dan menganalisis serangan DDoS (Distributed Denial of Service) menggunakan alat Wireshark dan Snort. Dalam konteks keamanan jaringan, serangan DDoS merupakan ancaman serius yang dapat menyebabkan gangguan signifikan pada infrastruktur jaringan. Penelitian ini dilakukan dengan merancang dan mengimplementasikan skenario serangan DDoS untuk memantau efektivitas Wireshark dan Snort dalam mendeteksi pola serangan. Hasil penelitian menunjukkan bahwa kedua alat tersebut mampu mengidentifikasi karakteristik dan pola serangan DDoS dengan akurasi yang tinggi. Wireshark menunjukkan kemampuannya dalam menangkap dan menganalisis paket data yang mencurigakan, sementara Snort efektif dalam memberikan peringatan dini tentang aktivitas mencurigakan yang terdeteksi. Dengan menggunakan metode ini, administrator jaringan dapat memperoleh wawasan yang lebih baik tentang sifat serangan dan mengembangkan strategi mitigasi yang lebih efektif. Penelitian ini memberikan kontribusi penting dalam pengembangan sistem deteksi intrusi yang lebih canggih dan dapat diandalkan untuk meningkatkan keamanan jaringan komputer.

Kata Kunci: DDoS, Keamanan Jaringan, Wireshark, Snort, Deteksi Serangan

ABSTRACT

Nama : Albilal Kahfi
NIM : 41520010008
Program Studi : Teknik Informatika
Judul Proposal Penelitian : Detection and Analysis of DDoS Attacks Using Wireshark and Snort
Pembimbing : Prof. Dr. Ir. Rahmat Budiarto

Detection and Analysis of DDoS Attacks Using Wireshark and Snort, This study aims to detect and analyze DDoS (Distributed Denial of Service) attacks using Wireshark and Snort tools. In the context of network security, DDoS attacks represent a serious threat that can cause significant disruptions to network infrastructure. The study was conducted by designing and implementing a DDoS attack scenario to monitor the effectiveness of Wireshark and Snort in detecting attack patterns. The results show that both tools are capable of accurately identifying the characteristics and patterns of DDoS attacks. Wireshark demonstrated its capability in capturing and analyzing suspicious data packets, while Snort proved effective in providing early warnings about detected suspicious activities. By utilizing this method, network administrators can gain better insights into the nature of attacks and develop more effective mitigation strategies. This study makes a significant contribution to the development of more advanced and reliable intrusion detection systems to enhance computer network security.

Keywords: DDoS, Network Security, Wireshark, Snort, Attack Detection.