

## INTISARI

### PROYEK AKHIR

#### **IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* BERBASIS SNORT DANGRAFANA DENGAN NOTIFIKASI TELEGRAM**

Perkembangan teknologi dalam jaringan yang pesat telah memberikan manfaat yang begitu besar pada masyarakat masa kini. Dengan adanya jaringan komputer dapat menghubungkan siapapun dimanapun dan kapanpun. Namun, semakin besar jaringan maka jaringannya akan semakin rumit. Koneksi antara jaringan yang semakin besar dapat meningkatkan resiko ancaman terhadap keamanan jaringan. Hal ini dapat menimbulkan masalah baru yang cukup mengancam keamanan jaringan. Ancaman yang dapat ditemukan antara lain *port scan*, *DoS*, dan lain sebagainya. Maka dari itu, jaringan harus terlindungi dari segala macam usaha penyusupan dan penyerangan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Salah satu solusi untuk menyelesaikan permasalahan tersebut yaitu dengan sistem monitoring pencegahan serangan atau *Intrusion Prevention System* (IPS) untuk memonitor dan melindungi jaringan dari serangan serta menganalisis jenis serangan. Snort diterapkan memantau lalu lintas data, menyimpan hasil deteksi dan melakukan *blocking* jika ada ancaman. Informasi yang diperoleh dari kegiatan penyusupan ditampilkan di *web monitoring* dan dikirimkan sebagai notifikasi menggunakan aplikasi Telegram. Selain itu, hasil log dapat dilihat melalui *web monitoring* sehingga tidak perlu mengakses *database* secara langsung.

Kata Kunci: *Intrusion Prevention System*, Keamanan Jaringan, Snort, Telegram

## ***ABSTRACT***

### ***IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM BASED ON SNORT AND GRAFANA WITH TELEGRAM NOTIFICATIONS***

The development of technology in the network has provided great benefits for today's society. With a computer network can connect anyone anywhere and anytime. However, the bigger the network, more complicated the network will be. Connections between networks that are getting bigger can increase the risk of threats to network security. This can cause new problems that are quite threatening to network security. Threats that can be found include port scans, DoS, FTP attacks, and so on. Therefore, the network must be protected from all kinds of intrusion attempts and attacks carried out by irresponsible parties. One solution to solve this problem is an attack prevention monitoring system or Intrusion Prevention System (IPS) to monitor and protect the network from attacks and analyze the types of attacks. Snort is implemented to monitor data traffic, save detection results and block if there is a threat. Information obtained from intrusion activities is displayed on the monitoring web and sent as notifications using the Telegram application. In addition, log results can be viewed through web monitoring so there is no need to access the database directly.

**Keywords:** Intrusion Prevention System, Network Security, Snort, Telegram