# Pengembangan host based intrusion detection system hbids dan analisa perbandingan kinerjanya dengan snort = Development of based host intrusion detection system hbids and its performance analysis against snort

Wisnu Broto, author



---

Abstrak

Pada dasarnya Intrusion Detection System (IDS) memonitor aktivitas lalu lintas jaringan yang mencurigakan, IDS merespon kejanggalan / anomaly lalu lintas jaringan yang dianggap berbahaya dengan melakukan tindakan seperti memblokir alamat Internet Protokol sumber intrusi. IDS mempunyai berbagai metode mendeteksi paket lalu lintas data yang mencurigakan, ada yang berbasis jaringan disebut Network Based Intrusion Detection System (NBIDS) dan yang lainnya berbasis host disebut Host Based Intrusion Detection System (HBIDS). HBIDS berbasis anomaly memonitor besarnya bandwidth, port dan protokol apa yang digunakan, pada paket lalu lintas data inbound dan outbound kemudian membandingkan pola paket lalu lintas data terhadap baseline HBIDS, bila terdeteksi terjadi anomaly dari perangkat jaringan akan mengirim alert kepada pengguna atau administrator untuk melakukan tindakan pencegahan terhadap intrusi jaringan. Simulasi ini mendapatkan data analisa kinerja HBIDS sebesar 18,56% lebih baik dari kondisi Snort.

.....Basically Intrusion Detection System (IDS) monitors network activity for suspicious traffic, the IDS responds to irregularities / anomalies of network traffic that is considered dangerous to perform actions such as blocking Internet Protocol address of the source intrusion. IDS has a variety of methods to detect packet data traffic is suspicious, there is a network-based so-called Network Based Intrusion Detection System (NBIDS) and the other so-called host-based Host Based Intrusion Detection System (HBIDS). HBIDS based anomaly monitors the amount of bandwidth, what ports and protocols used, the packet data traffic inbound and outbound packets then comparing traffic patterns against baseline data HBIDS, when the detected anomaly occurs from the network device will send alerts to the user or administrator to perform actions prevention against network intrusion. This simulation analysis of performance data HBIDS get for 18.56% better than the condition of Snort.