INTISARI

IMPLEMENTASI DAN ANALISIS PERBANDINGAN PERFORMA IDS SNORT DAN IDS SURICATA PADA RASPBERRY PI

Perkembangan internet yang pesat mendorong meningkatnya pengguna internet seperti pada saat ini. Penggunaan internet yang pada akhirnya menjadi kebutuhan hampir bagi setiap orang, namun hal ini menyebabkan siapa saja yang berperan sebagai pengguna internet menciptakan kerentanan pada sistem keamanan jaringan yang mereka miliki. Beberapa langkah preventif seperti penggunaan *firewall* untuk melindungi keamanan pada jaringan diharapkan dapat melakukan penyaringan berbagai ancaman pada jaringan. Namun pada akhirnya *firewall* juga memiliki keterbatasan untuk melakukan penangkalan serangan yang terjadi dari dalam jaringan itu sendiri. Maka dari itu diperlukan perlindungan untuk meningkatkan keaman jaringan yang dapat menutupi kekurangan dari *firewall* tersebut.

Intrusion Detection System (IDS) atau sistem deteksi intrusi dapat menjadi solusi dari kekurangan yang ada pada *firewall*, karena IDS dapat melakukan penyaringan paket data beserta isi dari paket di dalamnya. Terdapat beragam IDS yang sudah dikembangkan baik yang berbayar maupun *open source*. Produk *open source* dari IDS sendiri yang paling banyak digunakan saat ini adalah snort dan suricata. Pada penelitian proyek akhir ini dilakukan perbandingan kinerja diantara kedua IDS tersebut. Dari hasil penelitian ini didapatkan Pada pengujian performa dalam mendeteksi jumlah serangan IDS Suricata lebih baik dibanding IDS Snort karna berhasil medeteksi total 13 serangan berbanding dengan IDS Snort yang hanya mendeteksi 7 serangan. Dalam segi penggunaan *resource hardware* IDS Snort unggul dalam pemakaian CPU yang lebih rendah dibanding IDS Suricata, namun IDS Suricata unggul dalam penggunaan RAM. Sedangkan pada parameter pengujian waktu deteksi, IDS Snort hanya mampu mengungguli IDS Suricata lewat pengujian serangan shellcodes, untuk pengujian DOS IDS Suricata lebih unggul.

Kata Kunci : *Firewall*, IDS, Snort, Suricata, Pytbull, Raspberry Pi.

ABSTRACT

IMPLEMENTATION AND COMPARISON ANALYSIS OF IDS SNORT AND SURICATA IDS PERFORMANCE IN RASPBERRY PI

The rapid development of the internet has encouraged an increase in internet users as of now. The use of the internet is ultimately a necessity for almost everyone, but this causes anyone who acts as an internet user to create vulnerabilities in the network security systems they have. Some preventive steps such as the use of firewalls to protect security on the network are expected to be able to filter various threats to the network. But in the end the firewall also has limitations to counteract attacks that occur from within the network itself. Therefore protection is needed to increase the security of the network that can cover the shortcomings of the firewall.
Intrusion Detection System (IDS) or intrusion detection system can be a solution to the shortcomings that exist in a firewall, because IDS can filter data packets along with the contents of the package inside. There are various IDSs that have been developed both paid and open source. The open source product from IDS itself which is most widely used today is snort and suricata. In this final project research, a performance comparison was carried out between the two IDSs. From the results of this study, it was found that the performance test in detecting the number of IDS Suricata attacks was better than IDS Snort because it successfully detected a total of 13 attacks compared to IDS Snort which only detected 7 attacks. In terms of hardware resource use, IDS Snort is superior in lower CPU usage than Suricata IDS, but Suricata IDS is superior in RAM usage. Whereas in the parameters of testing the detection time, IDS Snort is only able to surpass the Suricata IDS by testing shellcodes attacks, for testing DOS IDS Suricata is superior.
.

***Keywords**: Firewall, IDS, Snort, Suricata, Pytbull, Raspberry Pi.*