Pengembangan portable Network Intrusion Detection System (nids) dengan open source IDS pada perangkat Raspberry Pi untuk infrastruktur jaringan skala kecil dan menengah = The development of portable Network Intrusion Detection System (NIDS) with Open Source IDS on Raspberry Pi for small and medium network infrastructure

Mochamad Zairy Fajar Ibrahim, author

Abstrak

Internet adalah hal yang sangat umum saat ini. Untuk memenuhi kebutuhan akses internet, banyak rumah maupun kantor yang memilih untuk menggunakan jaringan nirkabel karena fleksibilitasnya yang lebih baik dibandingkan dengan jaringan berkabel. Namun pada setiap jaringan selalu ada ancaman serangan yang dapat mengganggu konektivitas, hingga membahayakan perangkat dan data pengguna. Salah satu cara yang dapat digunakan untuk mendeteksi adanya serangan-serangan seperti ini adalah dengan menggunakan Intrusion Detection System (IDS) yang dapat memantau lalu lintas jaringan dan mendeteksi adanya aktivitas mencurigakan/berbahaya pada jaringan.
Pada penelitian ini, dilakukan pengembangan sistem IDS portable dengan menggunakan Raspberry Pi, sebagai solusi IDS yang terjangkau dan efektif untuk jaringan kecil dan menengah. Kemudian dilakukan perbandingan antara 2 jenis open source IDS, yaitu Snort dan Suricata. Hasil dari 2 skenario pengujian menunjukkan bahwa pada skenario 1, Snort berhasil mendeteksi 18 dari 20 serangan, dengan persentase penggunaan RAM 11.86% dan CPU 10.16%, serta waktu deteksi 203.92 detik. Sedangkan Suricata berhasil mendeteksi seluruh serangan, dengan persentase penggunaan RAM 8.44% dan CPU 13.07%, serta waktu deteksi 178.79 detik. Sementara itu, pada skenario 2, Snort berhasil mendeteksi seluruh serangan, dengan persentase penggunaan RAM 12.18% dan CPU 8.64%, serta waktu deteksi 72.6 detik. Sedangkan Suricata berhasil mendeteksi seluruh serangan, dengan persentase penggunaan RAM 7.96% dan CPU 13.5%, serta waktu deteksi 45.33 detik.
.....Internet is a very common thing nowadays. To fulfill the need of internet access, most of households and offices choose to use wireless network rather than wired network due to its better flexibility. However, regardless of the kind of network, there is always a threat of attacks which could disrupt the connectivity, and even harm the device or userâs data. One way to detect an attack to a network is by using Intrusion Detection System (IDS) to monitor the network traffic and to detect abnormal and dangerous activities.
.....This study is about a development of a portable IDS using Raspberry Pi, and two open source IDSs, Snort and Suricata, as a cost-efficient and effective portable IDS for small and medium network. The results of 2 test scenarios show that in scenario 1, Snort managed to detect 18 out of 20 attacks, with 11.86% RAM usage, 10.16% CPU usage, and detection time of 203.92 seconds. While Suricata managed to detect all the attacks, with 8.44% RAM usage and 13.07% CPU usage, and detection time of 178.79 seconds. Meanwhile, in scenario 2, Snort managed to detect all the attacks, with 12.18% RAM usage, 8.64% CPU usage, and detection time of 72.6 seconds. While Suricata managed to detect all attacks, with 7.96% RAM usage 13.5% CPU usage, and detection time of 45.33 seconds.<i/>