Evaluasi dan perbandingan kinerja sistem traffic monitoring dan sensor deteksi keamanan internet pada mata garuda, snort dan suricata = Performance evaluation and comparison of traffic monitoring system and internet security detection sensor of mata garuda snort and suricata/ Alvin Prayuda Juniarta Dwiyantoro

Alvin Prayuda Juniarta Dwiyantoro, author

Abstrak

Skripsi ini membahas tentang pengujian kapabilitas mesin deteksi dari IDS yang dikembangkan oleh ID-SIRTII, yaitu Mata Garuda dengan menggunakan framework Pytbull dan hasilnya akan dibandingkan dengan IDS lain yang sudah banyak didistribusikan di masyarakat dan bersifat open source, yaitu Snort dan Suricata. Pada skripsi ini akan dijelaskan mengenai konsep dasar dari IDS, berbagai macam bentuk serangan yang dapat menyerang jaringan, pengujian serangan pada Mata Garuda, Snort, dan Suricata, serta analisis hasil pengujian pada ketiga IDS tersebut.
Hasil pengujian menggunakan Pytbull yang dilakukan memberikan hasil bahwa akurasi deteksi Mata Garuda dan Snort secara keseluruhan (86.95%) lebih baik dibandingkan dengan Suricata (78.26%), namun dalam perbandingan ketepatan pendeteksian Suricata masih lebih unggul (73.91%) dibandingkan dengan Mata Garuda dan Snort (63.04%). Sedangkan dalam penggunaan resource CPU dan memori, Suricata lebih unggul dalam lingkungan multi core (40.67% pada core1 dan 5.39% pada core2, memori 919,917 bytes) daripada Mata Garuda (52.81% pada core1 dan 0.68% pada core2, memori 1,192,627 bytes) dan Snort (52.84% pada core1 dan 0.62% pada core2, memori 1,166,965 bytes).
.....
This research is concerned about the capability of detection engine from the IDS that developed by ID-SIRTII, called Mata Garuda using Pytbull framework and compared the result with the other well-known open source IDS, Snort and Suricata. This research will explain about the basic concept of IDS, some example of network attacks, penetration test to Mata Garuda, Snort, and Suricata, as well as the analysis about the result of the test from the three IDS.
The result of the test using Pytbull shows that the detection accuracy of Mata Garuda and Snort overall (86.95%) is better than Suricata (78.26%), but in the comparison of full detection ratio, Suricata (73.91%) is better than Mata Garuda and Snort (63.04%). In the comparison of CPU and memory usage, Suricata is better in multi core environment (40.67% on core1 and 5.39% on core2, memory 919,917 bytes) than Mata Garuda (52.81% on core1 and 0.68% on core2, memory 1,192,627 bytes) and Snort (52.84% on core1 and 0.62% on core2, memory 1,166,965 bytes).