Analisis Network Based Intrusion Detection Prevention System (NIDPS) menggunakan Suricata = Analysis of Network Based Intrusion Detection Prevention System (NIDPS) using Suricata

Pradana Angga Jatmika, author

Abstrak

NIDPS (Network-based Intrusion Detection Prevention System) merupakan sistem keamanan jaringan komputer yang mampu melindungi seluruh host yang ada dalam jaringan dengan cara mendeteksi dan melakukan pencegahan serangan sebelum sampai di host. Pada skripsi ini dilakukan implementasi NIDPS menggunakan Suricata. Suricata merupakan software IDS yang digunakan untuk melindungi host dengan cara mendeteksi serangan, sedangkan untuk menambahakan fitur pencegahan harus dilakukan konfigurasi pada fitur prevention Suricata dan firewall iptables. Pada skripsi ini akan dilakukan analisis terhadap NIDPS Suricata, meliputi fuctional tes, response time, pengaruh Suricata terhadap performansi jaringan berdasarkan parameter throughput, membandingkan 3 sistem keamanan jaringan yaitu Suricata, Honeyid, dan Ossec dan mencari detection rate dari Suricata. Hasil dari pengujian diperoleh bahwa untuk functional test, Suricata berhasil mendeteksi dan melakukan pencegahan terhadap serangan serta menampilkan serangan yang terjadi pada web-based interface Snorby. Hal ini dapat dilihat dari pengujian SYN flooding attack, Suricata berhasil mendeteski dan mendrop semua paket serangan SYN flooding. Pada pengujian response time, diperoleh response time Suricata untuk 1 serangan 0.015201 detik dan untuk 2 serangan sebesar 0.0435559 detik. Pada pengujian throughput diperoleh bahwa pemasangan Suricata tidak terlalu berpengaruh terhadap performansi jaringan. Perbandingan 3 sistem keamanan yaitu Suricata, Honeyid, dan Ossec, dimana Suricata memiliki rata-rata response time paling cepat dan Honeyd memiliki kemampuan deteksi paling baik dari beberapa pengujian serangan. Sedangkan Suricata kemampuan deteksinya (detection rate) yaitu 0.84 atau 84 % pada 12 pengujian serangan yang berbeda. ..... NIDPS (Network-based Intrusion Detection Prevention System) is a computer network security system that can protect all hosts on the network by detecting and preventing before the attack up to the host. This final project will be implemented NIDPS using Suricata. Suricata IDS is a software that is used to protect the host by detecting attacks, while adding features for prevention should be configured the prevention features Suricata and firewall iptables. In this final project will be conducted an analysis of Suricata, covering fuctional tests, response time, Suricata influence on network performance use throughput parameter, compare three network security system that is Suricata, Honeyid, and OSSEC and seek detection rate of Suricata. The results obtained from testing that for functional test, Suricata successfully detect and prevent attacks and show that the attack occurred on a web-based interface Snorby. It can be seen from the test SYN flooding attack, Suricata can detect and drop all SYN flooding attack packets. In the response time testing, the response time of Suricata is 0.015201 seconds for 1 attack and 0.0435559 seconds for 2 attack. In the throughput test, Suricata implemented does not affect significantly the network performance. Three comparative of the security system that is Suricata, Honeyid, and OSSEC, where Suricata has an average response time of the fastest and Honeyd has the best detection capability of several attempted attacks. While Suricata detection capability (detection rate) is 0.84 or 84% on testing 12 different attacks.