

Analisis honeyd low-interaction honeypot pada sistem keamanan jaringan = Analysis of honeyd low interaction honeypot in network security system

Ilyas Taufiqurrohman, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20387399&lokasi=lokal>

Abstrak

Salah satu sistem keamanan yang dapat diterapkan pada jaringan komputer adalah Honeypot. Honeypot merupakan sistem yang sengaja dijadikan umpan untuk menjadi target serangan dengan tujuan mengalihkan perhatian attacker dari sistem yang sesungguhnya. Pada jurnal ini dilakukan implementasi Honeyd: low-interaction Honeypot. Honeyd adalah sistem yang diset untuk meniru kegiatan dari sistem yang sesungguhnya dengan menggunakan virtual host. Virtual host tersebut dapat dikonfigurasi untuk meniru beberapa jenis services layaknya host maupun server pada jaringan komputer.

Pada jurnal ini dilakukan analisis terhadap Honeyd, meliputi functional test, responsive test, dan pengaruh Honeyd terhadap performansi jaringan berdasarkan parameter throughput, serta dilakukan perbandingan dengan sistem keamanan lain berupa Ossec dan Suricata.

Hasil dari pengujian diperoleh bahwa untuk functional test, virtual host Honeyd mampu meniru operating system dari host sebesar 99.61%. Dan untuk responsive test, diperoleh response time untuk Honeyd sebesar 0.0271 detik untuk 1 attacker dan 0.05439 detik untuk 2 attacker.

Berdasarkan pengujian juga diperoleh bahwa pemasangan Honeyd tidak berpengaruh terhadap performansi jaringan. Dan berdasarkan perbandingan antara Honeyd dengan Ossec dan Suricata, Honeyd memiliki keunggulan dalam hal melakukan deteksi terhadap serangan.

<hr><i>One effort that can be done in network security system is by implementing Honeypot. Honeypot is a system that is deliberately used as a bait to be the target of attacks from the attacker. The paper discusses implementation of Honeyd: Low-Interaction Honeypot. Honeyd is a system that is set up to mimic the activities of real system by using virtual hosts. Virtual hosts on Honeyd can be configured to mimic several types of services like host or server in a computer network.

In this paper is conducted the analysis of Honeyd, includes functional test, responsive test, and the effect of Honeyd in network performance based on throughput parameters, and also comparison between Honeyd, Ossec, and Suricata.

The results of functional test, Honeyd virtual host is able to mimic the operating system of the host by 99.61%. And for responsive test, response time for 1 attacker is 0.0271 seconds and response time for 2 attackers is 0.05439 seconds.

Based on the testing is also found that implementation of Honeyd does not significantly affect network performance. Based on the comparison between Honeyd, Ossec, and Suricata is found that Honeyd has advantages in attack detection tested.</i>