Analisis conpot low interaction honeypot sebagai sistem deteksi serangan pada jaringan industrial control system scada = Analysis of conpot low interaction honeypot as intrusion detection system in industrial control system scada network

Mahardianto Yudha Bestari, author

Abstrak

Pada skripsi ini akan dilakukan skema perancangan Conpot sebagai salah satu bentuk upaya peningkatan keamanan jaringan sistem ICS/SCADA. Maraknya penyerangan yang terjadi pada sistem SCADA yang terdapat pada industri-industri modern saat ini menarik perhatian bagi pengembang untuk memikirkan solusi dari masalah tersebut. Stuxnet adalah salah satu penyerangan malware kepada sistem SCADA yang sangat menggemparkan dunia perindustrian.
Honeypot merupakan salah satu teknologi sistem keamanan jaringan yang dapat diterapkan pada jaringan komputer dengan berbagai macam tujuan. Honeypot merupakan sistem yang sengaja dijadikan target serangan untuk mengalihkan perhatian attacker dari sistem sesungguhnya. Conpot akan disimulasikan dengan virtualisasi dari perangkat SCADA aslinya yaitu dengan menjalankan protokol yang ada pada sistem SCADA seperti Modbus TCP.
Berdasarkan analisis sistem dan hasil uji coba yang telah dilakukan, Conpot dapat menjadi salah satu solusi untuk meningkatkan keamanan sistem asli karena Conpot memiliki keandalan dalam mendeteksi serangan yang masuk kedalam jaringan modbus.
Hasil pengujian diperoleh bahwa untuk functional test, Conpot mampu meniru sistem PLC-SCADA. Pada responsive test, diperoleh response time sebesar 0.2521 detik untuk satu attacker dan 0.2582 detik untuk dua attacker. Berdasarkan pengujian juga bahwa pemasangan Conpot tidak berpengaruh terhadap performansi jaringan.
<hr>This thesis will do the Conpot design scheme as one of the effort to increase the SCADA network security system. Currently, the rise of the attack to the SCADA systems found in modern industries attracts the developer’s attention and trigger them to think of a solution to these problems. Stuxnet is one of the malware to attack SCADA systems which is appalling the world of industry.
Honeypot is one of the technology in network security system that can be applied to a computer network with a wide variety of purposes. Honeypot is a system that intentionally made to be a target of an attack in order to distract the attacker from the real system. Conpot will be simulated by virtualization from the real SCADA device, which is by running the protocol in SCADA system suchas Modbus TCP.
Based on the analysis of the system and the results of trials that have been done, Conpot can be a solution to improve the original system security because Conpot have the ability to detect the attacks into the Modbus network.
The test results showed that the functional test Conpot able to emulate PLC-SCADA systems. The result for responsive test, obtained response time of 0.2521 seconds for one attacker and 0.2582 seconds for two attackers. Based on testing also that the installation Conpot no effect on network performance.