Analisis dan implementasi deteksi keamanan jaringan menggunakan honeynet multiple sensor berbasis open-source = Analysis and implementation of detection in network security using multiple sensor honeynet based on open-source

Diyanatul Husna, author

Abstrak

Salah satu isu yang sangat penting dalam dunia internet saat ini adalah serangan-serangan dalam dunia maya dengan motivasi keuangan dan perangkat lunak berbahaya yang memiliki kemampuan untuk melakukan serangan secara otomatis. Honeypot dan IDS bekerja sama untuk memberikan solusi keamanan jaringan yaitu sebagai intrusion detection yang dapat mengumpulkan data serangan.
Pada penelitian ini, akan dibangun sistem keamanan jaringan menggunakan Honeynet multiple sensor yang berbasis open-source. Integrasi beberapa sensor Honeypot dan IDS dalam satu sistem disebut Honeynet. Honeypot dan IDS diimplementasikan pada suatu Host komputer dengan menggunakan MHN server sebagai web server, yang didalamnya dibangun sensor-sensor seperti Dionaea, Glastopf, Wortpot, p0f, Snort, dan Suricata.
Berdasarkan pengujian yang telah dilakukan diperoleh total keseluruhan alert yang berhasil direkam oleh sistem yaitu skenario 1: 5453 alert, skenario 2: 3021 alert, dan skenario 3:7035 alert dengan total keseluruhan serangan yaitu 15509 alert. Dari total keseluruhan serangan dideteksi 35% serangan berasal dari IP 192.168.1.103, 20% serangan berasal dari IP 192.168.1.104 , dan 45% serangan berasal dari IP 192.168.1.105.
Hasil pengujian ini menunjukkan bahwa sistem telah berhasil menjebak, memonitoring, dan mendeteteksi serangan. Pengimplementasian sistem Honeynet ini bertujuan agar kekurangan dari suatu sensor seperti halnya hanya dapat mendeteksi serangan terhadap port dan protocol tertentu dapat diatasi oleh sensor yang lain. Sehingga apapun bentuk serangan yang ada dapat dideteksi. Penggunaan Honeynet multiple sensor berbasis open-source dapat menjadi langkah awal yang baik untuk mitigasi resiko dan sebagai peringatan awal adanya serangan cyber.
<hr><i>Recently, some of the important issues in the internet things are the attacks in a network with profit motivation and malicious software which has the ability to do the attack automatically. Honeypot and IDS are working together to give the solution for network security and act as the instrusion detection which has the ability to collect the attack's log.
This research will build network security system using multiple sensor Honeynet based on open-source. The integration of Honeypot's sensors and IDS in one system is called Honeynet. Honeypot and IDS are implemented in a computer host using MHN server as the web server, that contains various of sensors such as Dionaea, Glastopf, Wortpot, p0f, Snort, and Suricata.
Based on the research that has been done, it showed total of alerts that is successfully recorded by system are for the first scenario, there are 5453 alerts, second scenario is 3021 alerts, and the third scenario is 7035 alerts with total of alerts are 15509. From the total attacks, it is detected that 35% of the attacks are from IP address 192.168.1.103, 20% are from IP 192.168.1.104, and the 45% are from IP 192.168.1.105.
This testing result showed that the system successfully monitores and detected the attacks. The purpose of

this implementation of Honeynet system is that one sensor can be able to handle another sensor's lack of ability, such as that can only detect the attack to the particular port and protocol. So, it can detect all various of attack. The application of Honeypot multiple sensors based on open-source could be the first step for the risk mitigation and acts as the first alert for the possibility of attack.</i>