

ABSTRAK

Arsitektur keamanan harus mendukung keadaan sistem yang terdiri dari komponen yang aman, komunikasi yang aman, dan kontrol akses aset yang aman ke setiap dan semua aset dalam ekosistem IoT (*Internet of Things* yang sedang dipertimbangkan). Keamanan ini terdiri dari beberapa aspek, yang terutama adalah keamanan data yang berada pada server. Beberapa penelitian sebelumnya yang dijadikan rujukan referensi utama membahas beberapa permasalahan terkait keamanan pada server IoT dan membahas keamanan pada web dengan beberapa tools yang berbeda. Berdasarkan rujukan tersebut, tercipta ide penelitian untuk melakukan Analisis Kerentanan Pada Jaringan IoT Menggunakan Raspberry Pi dan Owasp (*Open Web Application Security Project*).

Penerapan skema pengamanan jaringan terhadap IoT menggunakan tools OWASP berhasil dilakukan dengan memasang tools OWASP pada perangkat Raspberry Pi yang memiliki keuntungan lebih fleksibel dalam penggunaan dibanding komputer personal. Setelah dilakukan serangan pada server jaringan lokal didapatkan 7 jenis kerentanan dan solusi perbaikannya, kemudian dilakukan tahapan solusi dan didapatkan 7 kerentanan pada server jaringan lokal.

Didapatkan tingkat kerentanan dengan level tertinggi adalah medium dan level terendah Low. Dapat disimpulkan bahwa kerentanan paling tinggi didapatkan pada tipe jaringan cloud hosting, dikarenakan terkoneksi dengan internet. Berbeda dengan jaringan lokal yang hanya terkoneksi secara *local area network*.

Kata Kunci : IoT, Owasp, Raspberry Pi

ABSTRACT

The security architecture should support the state of the system consisting of secure components, secure communications, and secure asset access control to any and all assets in the IoT (*Internet of Things*) ecosystem under consideration. This security consists of several aspects, the main of which is the security of data residing on the server. Some of the previous researches that were used as the main reference discussed several security-related issues on IoT servers and discussed security on the web with several different tools. Based on these references, a research idea was created to conduct Vulnerability Analysis on IoT Networks Using Raspberry Pi and Owasp (*Open Web Application Security Project*).

The implementation of the network security scheme for IoT using the OWASP tool was successfully carried out by installing OWASP tools on Raspberry pi devices which have the advantage of being more flexible in use than personal computers. After an attack on a local network server, 7 types of vulnerabilities and solutions for repairs were obtained, then the solution stage was carried out and vulnerabilities were obtained on the local network server.

The highest level of vulnerability is medium, and the lowest level is low. It can be concluded that the highest vulnerability is obtained in the type of cloud hosting network, because it is connected to the internet. Unlike the local network which is only connected to the local area network.

Keywords : IoT, Owasp, Raspberry Pi

MERCU BUANA