Implementasi Aplikasi Berbasis Web Sebagai Sistem Pendeteksi Rogue Access Point dengan Wired-Side Solution

---

Abstrak

Rogue Access Point (RAP) menjadi salah satu ancaman dalam keamanan jaringan Wireless Local Area Network (WLAN) . RAP merupakan perangkat yang menciptakan sebuah jaringan wireless yang tidak dilegitimasi oleh network admin jaringan tersebut. Beberapa metode digunakan untuk mendeteksi RAP, yaitu berbasis hardware misalnya : perangkat sensor khusus untuk mendeteksi keberadaan RAP dan berbasis software, misalnya dibuatnya sistem berbasis aplikasi yang mampu mendeteksi RAP seperti sistem aplikasi berbasis web ini. Ada 2 bentuk model yang dapat terciptanya perangkat RAP yaitu RAP Unauthorized AP, RAP Bridging Connection. Sistem ini menggunakan 3 parameter yaitu IP, MAC Address dan Round Trip Time (RTT). Parameter ini menjadi penentu terdeteksinya suatu perangkat palsu yang termasuk RAP dalam skala satu jaringan. ketiga parameter itu akan diukur dengan cara membandingkan antara legal dan illegal. Perangkat yang legal telah didaftarkan oleh network admin kemudian melakukan deteksi terhadap jaringan tersebut, setelah itu dilakukan komparasi antara kedua data tersebut, perangkat yang tidak terdifinisikan dalam database merupakan perangkat yang ilegal. Sistem akan memberikan output berupa alarm dalam website. Dari hasil pengujian bahwa, waktu rata-rata Load Time yang dibutuhkan 5213.5569 milidetik untuk mendeteksi satu jaringan. Selain itu, juga diketahui bahwa tingkat akurasi sistem untuk model unauthorized AP sebesar 53,3% , sedangkan model Bridging Connection sebesar 90% mampu mendeteksi secara sempurna.

<hr>

Abstrak

Rogue Access Point (RAP) is one network security threat in Wireless Local Area Network (WLAN). RAP is a device that creates a wireless network that is not legitimized by admin network. Some of the methods used to detect RAP, which is based on hardware such as sensor devices for detecting and RAP-based on software, for example detection system that can detect RAP applications such as web-based application systems. There are two model that RAP-Unauthorized AP and RAP-Bridging Connection. This system uses three parameters, IP, MAC Address and Round Trip Time (RTT). This parameter determines the detection of a prosthetic device that includes a RAP-scale networks. All parameter will be compare between legal and illegal device. Legal devices that have been registered by the network admin and then perform detection on the network, after that, it carried out a comparison between the data, the device is not in the database, It mean that an illegal device. The system will give alarm output from the website. From the results of that testing, the average time needed 5213.5569 milliseconds Load Time to detect a network. In addition, it is also known that the accuracy of a model system for unauthorized APs of 53.3%, while the Connection Bridging the model is able to detect 90% perfectly.