Universitas Indonesia Library >> UI - Tesis Membership

Analisa kinerja sistem pendeteksi dan auto response rogue access point berbasis firewall pada model unauthorized AP = Performance analysis of rogue access point detection and auto response system based on firewall for model unauthorized ap

Adityo Abdi Nugroho, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=20349213&lokasi=lokal

---

Abstrak

Rogue Access Point (RAP) menjadi salah satu ancaman dalam keamanan jaringan Wireless Local Area Network. Salah satu RAP bermodel Unauthorized AP yaitu RAP terkoneksi dalam jaringan melalui kabel secara ilegal. Deteksi terhadap keberadaan RAP sudah banyak dikembangkan dengan berbagai metoda, menggunakan hardware atau software. Dengan sistem pendeteksi Rogue Access Point dan auto response, RAP akan secara otomatis dideteksi dan di blocking, sehingga akses RAP akan terhenti. Selain itu, Sistem Deteksi RAP menggunakan aplikasi berbasis web yang mempermudah network administrator dalam mengoperasikan aplikasi ini. Sistem ini menggunakan 2 parameter penting untuk mendeteksi yaitu IP dan MAC Address serta memberikan respon ke firewall untuk blocking.
Dari hasil percobaan sistem pendeteksi RAP dan auto response, kehandalan sistem mendeteksi dan auto response RAP mencapai sebesar 92,5% hingga 100% pada 1 RAP, 88,75 % hingga 95% pada 2 RAP, 93,33% hingga 96,67% pada 3 RAP dan 95% hingga 97,5% pada 4 RAP dengan 2 variasi mode yaitu manual dan otomatis. Selain itu, waktu rata-rata pendeteksian dan auto response mencapai 6,97 detik (1 RAP) waktu tercepat dan 18,79 detik (4 RAP) waktu terlama.
.....Rogue Access Point is one of network security threats in Wireless Local Area Network. One of type RAP are models Unauthorized AP which RAP may connect to the network cable or wireless illegally. RAP detection system has been developed with variety of methods, using hardware or software rogue access point detection system and auto response. The rogue access point will be automatically detected and blocked, so that RAP stops communicating with the network. In addition, RAP Detection system and auto response using the web-based application that facilitates the operation of the network administrator to configure. This system uses two important parameters to iterately detect the IP and MAC address and then give the "trigger" to the firewall for blocking action.
The results of experiment shows that system reliability to detect and to response against RAP reaches 92.5% to 100% on 1 RAP, 88.75% to 95% on 2 RAPs, 93.33% to 96.67% on 3 RAPs and 95 % to 97.5% on 4 RAPs with 2 variations modes : manual and automatic. and the average time detection and auto fastest response time reaches 6.97 sec (1 RAP) and the longest time to reaches 18.79 seconds (4 RAPs).