RANCANG BANGUN ZERO-TRUST WIFI ACCESS MENGGUNAKAN WPA3-SAE, RADIUS, DAN CAPTIVE PORTAL PADA JARINGAN LABORATORIUM TEKNIK INFORMATIKA POLBENG

Nama Mahasiswa : Petra Natanael Sinaga

NIM : 6103230022

Dosen Pembimbing : Lipantri Mashur Gultom, S.Kom, M.Kom

Abstrak

Keamanan jaringan nirkabel merupakan aspek penting dalam mendukung aktivitas akademik di Laboratorium Teknik Informatika Politeknik Negeri Bengkalis. Sistem keamanan yang masih menggunakan metode WPA2-PSK memiliki kelemahan karena menggunakan kata sandi bersama sehingga sulit mengidentifikasi pengguna secara individual dan rentan terhadap penyalahgunaan akses. Penelitian ini bertujuan merancang dan mengimplementasikan sistem *Zero-Trust WiFi Access* dengan mengintegrasikan WPA3-SAE, RADIUS, dan *Captive Portal* untuk meningkatkan keamanan jaringan laboratorium. Metode penelitian yang digunakan adalah penelitian terapan dengan pendekatan rekayasa sistem yang meliputi analisis kebutuhan, perancangan topologi jaringan, implementasi konfigurasi perangkat, pengujian *autentikasi*, pengujian AAA (*Authentication, Authorization, Accounting*), pengujian prinsip *least privilege*, *monitoring* aktivitas pengguna, serta pengujian terhadap serangan *brute force*, *sniffing*, DDoS, dan *Rogue Access Point*. Hasil implementasi dan pengujian menunjukkan bahwa sistem berhasil menerapkan autentikasi berlapis sesuai konsep *Zero Trust*, di mana setiap pengguna harus melalui proses verifikasi serta pembatasan hak akses secara individual melalui integrasi WPA3-SAE, RADIUS, dan *Captive Portal*. Seluruh aktivitas pengguna tercatat secara terpusat pada *log* sistem, serta prinsip *least privilege* mampu diterapkan sesuai kebijakan jaringan laboratorium. Pada pengujian keamanan, sistem terbukti tangguh dalam menolak upaya *brute force*, menjaga kerahasiaan data dari ancaman *sniffing* melalui enkripsi WPA3-SAE, mempertahankan ketersediaan layanan saat terjadi serangan DDoS, serta mencegah perangkat pengguna terhubung ke *Rogue Access Point*. Berdasarkan hasil pengujian tersebut, sistem mampu meningkatkan keamanan jaringan WiFi dibandingkan metode WPA2-PSK, mengurangi risiko akses ilegal, serta mempermudah administrator dalam melakukan pengelolaan dan pemantauan jaringan. Dengan demikian, penerapan *Zero-Trust WiFi Access* layak digunakan sebagai solusi peningkatan keamanan jaringan nirkabel di Laboratorium Teknik Informatika Politeknik Negeri Bengkalis..

Kata Kunci: *Zero-Trust Security*, WPA3-SAE, RADIUS, *Captive Portal*, Keamanan WiFi.

DESIGN AND IMPLEMENTATION OF ZERO-TRUST WIFI ACCESS USING WPA3-SAE, RADIUS, AND CAPTIVE PORTAL IN THE COMPUTER ENGINEERING LABORATORY NETWORK OF POLITEKNIK NEGERI BENGKALIS

Student Name : Petra Natanael Sinaga

Student ID Number : 6103230022

Academic Supervisor : Lipantri Mashur Gultom, S.Kom., M.Kom

Abstrack

Wireless Local Area Network (WLAN) security is a crucial aspect of supporting academic activities in the Informatics Engineering Laboratory at Politeknik Negeri Bengkalis. The existing security system utilizing the WPA2-PSK method has vulnerabilities due to its reliance on a shared password, making individual user identification difficult and leaving the network prone to access abuse. This research aims to design and implement a Zero-Trust WiFi Access system by integrating WPA3-SAE, RADIUS, and a Captive Portal to enhance the laboratory network security. The research methodology employed is applied research with a systems engineering approach, which includes requirements analysis, network topology design, device configuration implementation, authentication testing, AAA (Authentication, Authorization, Accounting) testing, least privilege principle testing, user activity monitoring, as well as security testing against brute force, sniffing, DDoS, and Rogue Access Point attacks. The implementation and testing results demonstrate that the system successfully applies layered authentication aligned with the Zero Trust concept, where every user must undergo verification and individual access rights restriction through the integration of WPA3-SAE, RADIUS, and the Captive Portal. All user activities are logged centrally within the system, and the least privilege principle is effectively enforced according to the laboratory network policy. In security testing, the system proved resilient by repelling brute force attempts, maintaining data confidentiality against sniffing threats via WPA3-SAE encryption, preserving service availability during DDoS attacks, and preventing user devices from connecting to Rogue Access Points. Based on these test results, the system enhances WiFi network security compared to the conventional WPA2-PSK method, reduces the risk of unauthorized access, and simplifies network management and monitoring for administrators. Therefore, the implementation of Zero-Trust WiFi Access is viable as a solution to enhance wireless network security in the Informatics Engineering Laboratory at Politeknik Negeri Bengkalis.

Keywords: Zero-Trust Security, WPA3-SAE, RADIUS, Captive Portal, WiFi Security.