ABSTRAK

Dewasa ini kemajuan teknologi sangatlah pesat. Salah satu faktor penyebabnya adalah meningkatnya modernisasi dan penggunaan dari jaringan internet. Apalagi era *Internet of Things* (IoT) sudah dimulai, dimana komunikasi terjadi antara mesin (*m2m communication*) dengan sedikit atau tanpa andil tangan manusia lagi. Tidak heran jika hamper semua orang memiliki akses internet masing-masing di rumah , perkantoran, atau tempat publik lain. Majunya teknologi saat ini, memungkinkan kita terhubung ke internet secara nirkabel. Kali ini penulis akan membahas *Wireless Fidelity* (Wi-Fi) *networks*. Banyak sekali pengguna Wi-Fi yang ada di dunia saat ini. Namun, kemajuan teknologi ini tentunya tak luput dari resiko dan masalah. Salah satu resiko atau masalah pada jaringan Wi-Fi adalah terdapatnya *attacker* yang kejahatannya berkaitan dengan *cyber crime* (theft identity, phising, dll). Oleh karena itu teknologi ini juga memiliki sistem keamanan tersendiri. Salah satunya dalam bentuk *gateway*.

Gateway yang penulis bahas adalah *captive gateway*, dimana pengguna Wi-Fi akan menjumpai suatu bentuk otentikasi dalam bentuk *web authentication*. *Web Authentication* pada umumnya masih menggunakan cara konvensional dengan cara menuliskan *pre-assigned* data seperti *username* dan *password* pada kolom yang disediakan. Cara otentikasi seperti ini memiliki resiko yaitu adanya *social engineering* seperti seorang *attacker* dengan mudah melihat jari-jari kita saat mengetikkan *username* dan *password* kita, sehingga attacker tersebut juga mendapatkan akses.

Dalam penelitian kali ini, penulis mengusulkan metode otentikasi berupa *captive gateway* berbasis *barcode scanner*, dengan menggunakan *router* MikroTik, dan *JavaScript* untuk mewujudkan *captive gateway*-nya. Hasil penelitian ini akan memungkinkan pengguna melakukan otentikasi tanpa harus mengetikkan kredensial-kredensial pengguna. Pengujian pada sistem yang digunakan dilakukan pada 3 *device* dengan tes skenario berupa perbedaan jarak (10, 15, 20 cm) antar kamera dan *barcode*. Hasil yang didapat berupa probabilitas keberhasilan dalam mendeteksi *barcode,* dengan probabilitas paling besar 96,67% saat menggunakan *device* dengan kamera 16 *megepixel* (mp) dengan jarak pengujian 10 cm, dan paling

kecil 40% saat menggunakan *device* dengan kamera 8 mp dengan jarak pengujian 20 cm. *Device* ke-3 dengan kamera 2 mp tidak mendapatkan hasil dikarenakan kurangnya dukungan *javascript* pada *device* tersebut.

Kata Kunci : *Captive Portal*, *Web Authentication*, JavaScript, QuaggaJS, MikroTik,