INTISARI

Percepatan laju teknologi yang pesat menyebabkan peningkatan kejahatan siber, termasuk pemanfaatan jaringan Wi-Fi sebagai perantaranya. Survei lapangan menunjukan 2 dari 7 orang pernah menjadi korban kejahatan siber karena terhubung dengan jaringan Wi-Fi publik. Penelitian ini yang berjudul "Analisis Keamanan Jaringan Wi-Fi Publik terhadap Pengguna melalui Penerapan Pemindai Kerentanan dengan Metode Security Policy Development Life Cycle" bertujuan untuk mencari celah kerentanan di jaringan Wi-Fi publik @FreeBiznetHotspot di Alun-alun Purwokerto. Dengan menggunakan tool pemindai kerentanan Nessus ditemukan 24 celah kerentanan yang terdiri dari 1 skala medium, 2 skala low, dan 21 skala informational. Dan pada tool Acunetix ditemui 6 celah kerentanan dengan skala 1 medium, 1 low, dan 4 informational. Melalui konfigurasi pada perangkat pengguna, celah kerentanan dengan skala medium berhasil dihindari tanpa mengurangi pengalaman pengguna dalam menggunakan jaringan Wi-Fi publik. Hasil penelitian ini menunjukkan bahwa penggunaan tool Nessus dan Acunetix dapat secara efektif mendeteksi celah kerentanan yang membahayakan pengguna dari kejahatan siber melalui penggunaan jaringan Wi-Fi publik.

Kata kunci: SPDLC, nessus, acunetix, wi-fi publik, kerentanan

ABSTRACT

The rapid pace of technological advancement has led to an increase in cybercrime, including the exploitation of Wi-Fi networks as a medium. Field surveys show that 2 out of 7 people have fallen victim to cybercrime due to connecting to public Wi-Fi networks. This research, titled "Analysis of Public Wi-Fi Network Security for Users through the Application of Vulnerability Scanners Using the Security Policy Development Life Cycle Method," aims to identify vulnerabilities in the @FreeBiznetHotspot public Wi-Fi network at Alun-alun Purwokerto. Using the Nessus vulnerability scanner tool, 24 vulnerabilities were found, consisting of 1 medium scale, 2 low scale, and 21 informational scale. With the Acunetix tool, 6 vulnerabilities were detected, consisting of 1 medium scale, 1 low scale, and 4 informational scale. By configuring user devices, the medium-scale vulnerability was successfully avoided without compromising the user experience when using the public Wi-Fi network. The results of this study indicate that the use of Nessus and Acunetix tools can effectively detect vulnerabilities that endanger users from cybercrime through the use of public Wi-Fi networks.

Keywords: SPDLC, nessus, acunetix, public wi-fi, vulnerability