Abstract

The increasing human need for Internet access requires Internet access service that is easy to do as the availability of Wi-Fi hotspot. Among the many Wi-Fi hotspots in public service locations in Yogyakarta is still very little attention to the security of data communications on the wireless network. This makes the hacker be interested to discover his ability to perform various activities of cybercrime. This study aims to analyze and test the Wi-Fi network security contained in locations of public services in Yogyakarta. The method used in this study is a qualitative method that consists of five main steps, namely the study of literature, the issue of criteria Wi-Fi, research instruments, data collection, and analysis. The location of public services, Wi-Fi hotspot providers selected in three categories: hotel, restaurant / cafe, and educational institutions. Each public service category taken sample 5 different locations. Testing is done with action that leads to crime by type of action such as sniffing, DNS spoofing and hijacking. The results showed that the majority of Wi-Fi located at the location of public service vulnerable to criminal attack. Wi-Fi throughout the studied (100%) are not secure against sniffing activities, 80% are not secure against DNS spoofing activities, and 66.6% are not
secure against hijacking action.

References


Index Terms

Computer Science Security

Keywords
Wi-Fi security, cybercrime, sniffing, DNS spoofing, hijacking