The 2nd Conference on Management, Business, Innovation, Education, and Social Science (CoMBInES)

Taichung, Taiwan 3-6 March, 2022

COMPARISON OF WPA2 EAP-PSK AUTHENTICATION SYSTEM ON WIRELESS NETWORK WITH PENETRATION TESTING METHOD USING FLUXION TOOLS

Stefanus Eko Prasetyo, Try Windranata
Faculty of Computer Science, Batam Internasional University, Indonesia
{ stefanus@uib.ac.id , 1831148.try@uib.edu }

ABSTRACT

Wireless Network is a collection of electronic devices that connect to each other using air devices or frequencies as a data traffic flow. Today, there are many users who use WPA2-PSK or WPA2-EAP as a wireless network security system that aims to prevent people from accessing it without permission. This research uses a wireless penetration testing technique that uses fluxion tools by comparing and analyzing the WPA2 authentication security system with EAP-PSK on a wireless network which aims to determine the vulnerability of a network security system. To carry out penetration testing, the author refers to the "Wireless Network Penetration Testing Methodology." Which consists of intelligence gathering, vulnerability analysis, threat modeling, password cracking, and reporting. From this study, it will be concluded that WPA2-PSK is less safe to use because it can be seen in the penetration testing that WPA2-PSK was successfully hacked in an unhide SSID state, while WPA2-EAP was successful in making Web Interfaces but failed to obtain information such as usernames and passwords. If the WPA2-PSK SSID is in a hide state, it will fail the hack, so that both security systems have their own advantages and disadvantages depending on the user's needs.

Keyword: *Penetration Testing, Fluxion Tools, WPA2-PSK, WPA2-EAP, Wireless Network*