ABSTRACT

ANALYSIS OF WIRELESS LAN NETWORK SECURITY USING THE NIST 800-115 STANDARD (CASE STUDY ON A CAFE IN BANDUNG)

By

Setya Budi Pradana

1202170168

Technological developments that are increasingly developing, there is a technology that is easy to use and has been widely implemented, namely Wi-Fi. However, there are vulnerabilities in Wi-Fi networks caused by their wireless. Therefore, this study was made to conduct testing and security analysis on public Wi-Fi networks in three cafes in the city of Bandung, namely cafe X, cafe Y, and cafe Z using standard NIST 800-115. NIST 800-115 contains four successive stages, namely the planning stage to plan targets and objectives, the discovery stage to collect information and analyze vulnerabilities, the attack stage to perform attack testing, and the last stage is the reporting stage, which is to report the results and provide suggestions regarding vulnerabilities. At the attack stage, several attack tests were carried out such as unauthorized access, DoS attacks, telnet attacks, and packet sniffing. Based on the results of the analysis and tests that have been carried out on each cafe, each attack was successful. The unauthorized access attack was successfully carried out using the default username password to log in as admin, the DoS attack succeeded in disconnecting and making the users of the Wi-Fi network unable to reconnect, the telnet attack was successful in capturing telnet packets, and finally packet sniffing succeeded in obtaining information on activities carried out by Wi-Fi network users. The test results show that every Wi-Fi network is vulnerable to attack and needs to be repaired by changing the default username password, configuring the firewall, turning off and changing the telnet protocol, and always updating the device system.

Keywords— Wi-Fi, network security, NIST 800-115, Vulnerability Analysis, Penetration Testing