ABSTRACT

WEAKNESS ANALYSIS AND SECURITY TESTING OF WIRELESS LAN NETWORKS USING PENETRATION TESTING EXECUTION STANDARD (PTES) (CASE STUDY ON CAFES IN PALEMBANG)

By

FAIRUZ ZAHIRAH LIDANTA

1202174084

The need for the internet has influenced information delivery in social life. Currently, accessing the internet is very easy by simply connecting to a Wireless LAN network. Wireless Local Area Network (WLAN) is a computer network that transmits data using radio waves, another form of WLAN network is Wi-Fi. Wi-Fi is publicly available and is accessible such as in cafes, but few pay attention to its safety. Therefore, testing is needed to evaluate network security in cafes to anticipate unwanted things to happen. This can be done by various methods, such as implementing Vulnerability Assessment and Penetration Testing (VAPT) based on the Penetration Testing Execution Standard (PTES). PTES is a standard used to perform test simulations with sequential stages from information gathering to reporting results to be easy to understand. Information and vulnerabilities found in each cafe would be analysed and conducted testing simulation. This study research showed several Unauthorized Access, DoS attack, Telnet attacks, and Packet Sniffing tests applied to the three cafes. After testing is conducted, we got some vulnerability information, such as successfully accessing the website using the default username and password, disconnecting the network, capturing data packets, and get a telnet username and password. The testing results show that the security of the WLAN network still has vulnerabilities that can exploit. Based on this research, the results of Unauthorized Access testing, DoS attacks and packet sniffing were all successfully carried out in the three cafes. However, the telnet attack only succeeded in two cafes, namely Cafe A and Cafe C. This research is expected to increase awareness of information security for both cafe managers and cafe users to minimize attacks that can occur when using public Wi-Fi.

Keywords – ***WLAN, PTES, wireless security, vulnerability analysis, penetration testing, security attacks***