# ABSTRACT

Bobby Irwanda (0832004007)

## Wi-Fi Protected Access (WPA) Hacking

## Using BackTrack 2

(xxiii+143 pages, 6 tables, 84 figures, 4 appendices)

The improvement of computer technology causes the development of computer networking technology improves. Now, the computer networking is moving away from wired networking to the wireless networking. This movement not only gives a lot of advantages to the users but also brings possible weaknesses which are prone to attacks. One of them is about the security of the network. The security of wireless network is not as good as the wired network, because of that many efforts had been done by implementing better security policy. One of the wireless security protocol is Wi-Fi Protected Access (WPA). This protocol is the successor of Wired Protected Access (WEP). This replacement was made to fix the weaknesses in WEP, but WPA also have some weaknesses which have been exploited by hackers too.

This final project presents the exploitation of WPA's weaknesses. The exploitation will start from the wireless network sniffing activity, capturing the handshaking package, creating a dictionary file, translating the pre-shared key and finally using the decrypted key to enter the network. This final project also gives some preventive actions to minimize the probability of network for being hacked. The prevention action is made from the analysis of the attack which were done in this research.

Finally to minimize the possibility from being hacked by using WPA, there are some solutions like using choosing a good pre-shared key, and changing the pre-shared key periodically. The solutions cannot insure the network is free from hacking, but they will reduce the probability from being hacked successfully and increase the time required for a hacker to hack user's WLAN.

References : 20 (2003-2008)