

ABSTRACT

In fact actually the term of wirelessLAN technology is not a new matter, but the hoisterous of technological use of wirelessLAN is newly just felt latterly. Nowadays a lot of ISP build wireless infrastructure in performing its service, internal communications of company also using wirelessLAN . this technology use the frequency 2,4 Ghz which have been freed its use by government, hence because it free this 2,4 Ghz band is not protected judicially which ironically exactly is used by a lot of company for the communications of the company. Because is not protected by the law hence this 2,4 Ghz band also do not fulfill the security standart like for example at frequency 800/900/1800 Mhz (cellphone) so that this matter become like a sitting duck to all hacker to infiltrate and steal at the network.

In this final project, an analysis will be conducted to test the security system of wirelessLAN, by doing an activity called wardriving. Wardriving represent the scanning activity. Wardriving conducted by using notebook provided with a wireless NIC wich support the promiscuous mode to tap the wirelessLAN signal. Hereinafter by using certain tools can be jointed to a protected wirelessLAN to infiltrate into the network to steal ex. certain company secret because wirelessLAN is also used by company in braiding internal communications of the company or to get(“steal”) the internet access anonymously.

To be expected in this final project is to know whether the security system of wirelessLAN that exist in in this time can protect itself from the infiltration attack.

Keywords : wardriving, wirelessLAN, promiscuous(monitor) mode, security system