ABSTRAK

Keamanan data sebuah perusahaan adalah suatu hal yang sangat penting, maka diperlukannya keamanan untuk menjaga data-data penting tersebut agar tidak disalahgunakan. Salah satu celah yang dapat diserang ialah jaringan nirkabel karena dapat terlihat oleh publik. Pada PT. Gerak Puncak Lancar sendiri mempunyai jaringan nirkabel untuk akses internet karyawannya. Penelitian ini bertujuan untuk menguji seberapa kuat sistem keamanan dari perusahaan tersebut dengan metode Penetration Test ISSAF. ISSAF merupakan sebuah framework standard pengujian Penetration Test untuk berbagai keamanan. Seperti keamanan WLAN, website, keamanan Router, keamanan Firewall dan lain-lainnya. ISSAF sendiri mempunyai 9 aktivitas atau langkah meliputi Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access & Privilage Escalation, Enumerating Further, Compromise Remote User/Sites, Maintaining Access dan Covering tracks. Untuk Wlan Security Assessment sendiri mempunyai 6 tahap yakni, Information Gathering, Scanning, Audit, Analysis & Research, Exploit & Attacks, Reporting & Presentation. Hasil analisa penelitian ini, keamanan jaringan nirkabel Access Point staff PT. Gerak Puncak Lancar. Mempunyai nilai Overall Risk Rating tinggi atau High. Evaluasi pun dilakukan pada keamanan jaringan PT. Gerak Puncak Lancar, dan hasil evaluasi tersebut menurunkan Overall Risak Rating menjadi Medium.

Kata Kunci : Uji Penestrasi, ISSAF, WLAN, Keamanan Jaringan, Aircrack-ng

ABSTRACT

The security of a company's data is highly important, requiring measures to protect the crucial information from potential misuse. One vulnerability lies in the wireless network, which can be visible to the public. PT. Gerak Puncak Lancar has its own wireless network for its employees' internet access. This research aims to assess the strength of the company's security system using the ISSAF Penetration Test method, a standard framework for testing various security aspects like WLAN, website, router, firewall, and more. ISSAF involves 9 activities, including Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access & Privilege Escalation, Enumerating Further, Compromising Remote Users/Sites, Maintaining Access, and Covering Tracks. The WLAN Security Assessment has 6 stages: Information Gathering, Scanning, Audit, Analysis & Research, Exploit & Attacks, and Reporting & Presentation. The research analysis results indicate that the wireless network security of PT. Gerak Puncak Lancar's staff Access Point has a high Overall Risk Rating. An evaluation was conducted on the network security of PT. Gerak Puncak Lancar, and the evaluation results lowered the Overall Risk Rating to Medium.

Keywords : Pentest, ISSAF, WLAN, Network Security, Aircrack-ng