BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian penetrasi yang dilakukan dengan menggunakan metode PTES (Penetration Testing Execution Standard), antara lain teknik exploiting, scanning, nmap, sniffing, arp spoofing, dan cracking enkripsi. Sebagai hasil dari ini, dapat disimpulkan bahwa:

1. Kerentanan yang harus diwaspadai yang dapat diserang oleh *attacker* merupakan kerentanan *Cracking the encryption, Arp Spoofing, Sniffing, dan Bypassing Mac Address* yang memiliki tingkat kerentanan *sensitive data exposure High*
2. Dalam melakukan analisis keamanan jaringan wireless pada PT. QWE dengan metode *Penetration Testing Execution Standard* (PTES). Dalam tahapan awal yang dimana melakukan beberapa tahapan yang pertama adalah *Wireless Reconnaissance, Identify Wireless Networks, Vulnerability Research, Exploitation, Reporting, dan Remediation And Security Controls*. Yang dimana disetiap tahap tersebut sudah dilakukan dalam penelitian ini seperti melakukan persiapan dalam melakukan penyerangan dengan menidentifikasi ada berapa jaringan dan jenis keamanan dari jaringan wireless tersebut, mengecek kerentanan yang ada pada jaringan wireless dengan tools *nessus*, melakukan serangan setelah menentukan jenis kerentanan dan menghasilkan apasaja jenis kerentanan yang ada pada jaringan tersebut yang mungkin dapat membahayakan sebuah PT.QWE
3. Hasil dari pengujian penetrasi yang dilakukan dengan serangan *Sniffing* terhadap jaringan *Wireless* PT. QWE yang dimana menghasilkan sebuah kerentanan yang dapat membahayakan PT. QWE tersebut. Yang dimana peneliti mendapatkan sebuah akses MITM (*Man In The Middel*) yang memiliki arti dimana kita dapat

mendengarkan komunikasi dua arah yang dilakukan oleh korban dengan jenis serangan *Sniffing*.

Penemuan kerentanan tersebut membuktikan bahwa jaringan pada PT. QWE masih belum memenuhi komponen keamanan.

5.2 Saran

Berdasarkan uraian dari kesimpulan, maka kelebihan dan kekurangan diatas dapat menjadi pelajaran serta referensi untuk kedepannya. Saran-saran yang dapat dipertimbangkan untuk kedepannya antara lain :

1. Diperlukan pembagian jaringan agar dapat membedakan jaringan. yang nantinya apabila ada serangan tidak semua data dapat dicuri oleh *attacker*
2. Sebaiknya dilakukan penggantian *password* secara berkala untuk login untuk menghindari terjadinya penyusupan oleh pihak-pihak yang tidak bertanggung jawab.
3. Pengecekan jaringan secara berkala diperlukan untuk menghindari terjadinya permasalahan pada jaringan yang dapat menyebabkan kinerja jaringan menjadi lambat
4. Waspada terhadap kelemahan berbahaya yaitu *krackattacks* yang mungkin dalam melemahkan keamanan jaringan