BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis keamanan jaringan pada fasilitas internet terhadap serangan *system failure* pada toko services w-elektrik batam dapat diambil kesimpulan:

1. Identifikasi dilakukan menggunakan fitur SSID, *mac address*, RSSI, *vendor*, *channel* yang dipakai, *network type security* dan hasilnya didapatkan Wi-Fi yang berada di area penelitian ini pengaman tidak kuat.
2. Percobaan yang dilakukan berhasil diperoleh informasi mengenai akses DNS yang dituju dan peneliti juga mendapatkan *username* dan *password email* dari salah satu target dan menyimpulkan bahwa Wi-Fi yang ada di toko services w-elektrik batam tidak aman karena semua kegiatan dapat dengan mudah terekam dan mudah dicuri.

5.2 Saran

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

1. Buatlah jaringan yang tepat Sebelum memulai pemasangan jaringan, pertimbangkan apa yang akan lakukan dengan jaringan tersebut dan bagaimana akan digunakan. Ini akan membantu menentukan jenis jaringan

yang paling sesuai, seperti jaringan LAN (Local Area Network) atau WAN (Wide Area Network), serta jumlah dan jenis perangkat yang diperlukan.

2. Pastikan untuk mengamankan jaringan, Gunakan keamanan jaringan seperti firewalls dan enkripsi untuk melindungi jaringan dari serangan yang tidak diinginkan. Juga pastikan untuk membuat sandi yang kuat untuk semua perangkat jaringan.
3. Jaga agar jaringan terorganisir. Buatlah skema jaringan yang terstruktur dan terorganisir dengan baik, agar mudah untuk dikelola dan di troubleshoot jika terjadi masalah.
4. Pertahankan jaringan. Pastikan untuk selalu memperbarui perangkat jaringan dan menjalankan pemeliharaan rutin, seperti membersihkan konektor dan memeriksa kabel-kabel untuk menjaga kinerja jaringan tetap optimal.
5. Menggunakan AES dengan *key* yang panjangnya 8-63 karakter pada WPA2- PSK agar proses *crack* atau sadap yang dilakukan oleh pihak yang tidak bertanggung jawab, membutuhkan waktu yang lama. Sehingga kita dapat meng-*update* sistem keamanan sebelum orang bisa melakukan *crack* ataupenyadapan pada sistem jaringan *wireless*.