BAB V

PENUTUP

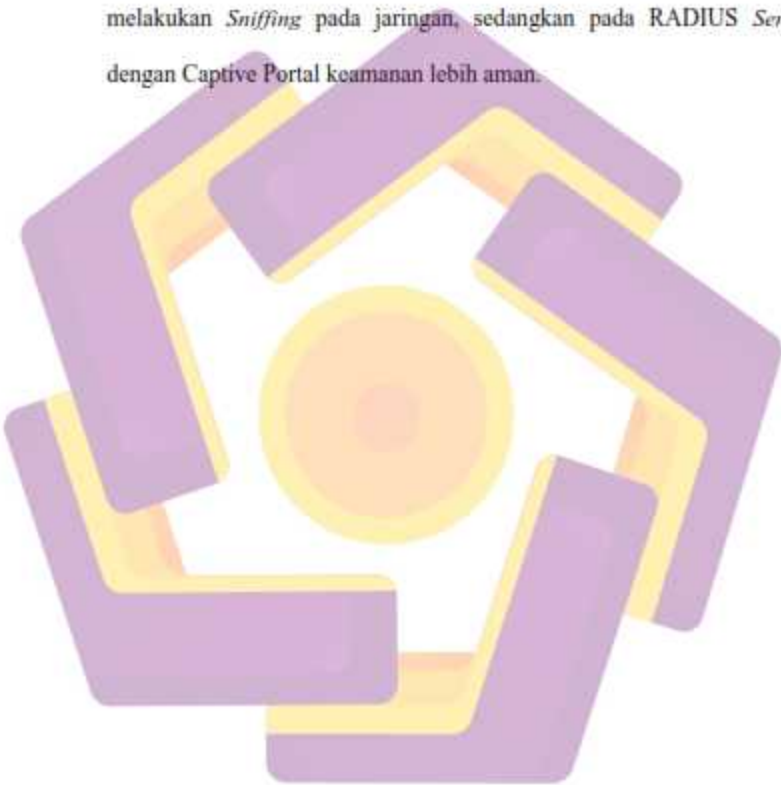
5.1 Kesimpulan

Berdasarkan hasil dari analisis dan pengujian tentang skripsi ini yang berjudul "ANALISI KEAMANAN WPA2-PSK DAN RADIUS SERVER MENGGUNAKAN METODE WIRELESS PENETRATION TESTING" dapat ditarik kesimpilan yaitu:

1. Pada sistem keamanan RADIUS Server memiliki enksripsi yang lebih bagus dibandingkan dengan WPA2-PSK karea hanya user yang terdaftar saja yang bisa masuk kedalam jaringan tersebut.
2. Dalam sistem keamanan RADIUS Server memeiliki tingkat keamanan yang labih baik karena beberapa percobaan pengujian mnegalami kegagalan.
3. WPA2-PSK memiliki enkripsi yang cukup kuat, namun apabila menggunakan *Password* atau *Passphrase* yang lemah masih memungkinkan untuk dilakukan proses *Cracking password* menggunakan *Brute Force.*
4. Sistem keamanan RADIUS *Server* dengan Captive Portal ini menawarkan alternatif keamanan pada jaringan *Wireless* LAN yang kuat, dan juga

manajement *User* yang terkontrol. Dari hasil pengujian menunjukan bahwa sistem ini sanggat sulit untuk dijebol menggunakan teknik *Brute Force, MAC Address spoofing,* dan *Main in the Midle.*

5. Keamanan data pada WPA2-PSK masih tergolong rendah karena data sensitif seperti *Username* dan *Password* dapat di ketahui dengan melakukan *Sniffing* pada jaringan, sedangkan pada RADIUS *Server* dengan Captive Portal keamanan lebih aman.



5.2 Saran

Setelah mengevaluasi dan membaca laporan penelitian ini, penulis menyadari bahwa masih banyak kekurangan dalam melakukan penelitian dan pengujian terhadap sistem ini, dengan kekuranagan tersebut penulis menuliskan beberapa saran yang mengukin dapat menjadi acuan atau dikembangkan untuk penelitian kedepanya:

1. Apabila masih mengunakan sistem keamanan WPA2-PSK gunakan Password dan username yang lebih sulit misal menggunakan password "abcd#$*123^^" agar Brute force kesulitan unutuk menemukan atau malacak password pengguna jaringan *Wireless*.
2. Untuk mendapatkan jaringan *Wireless* yang lebih aman, gunakan RADIUS *Server* dengan otentikasi Caprive Portal yang bia mengurangsi resiko-resiko yang tidak diinginkan.
3. Pada pengujian ini hanya mengunakan 5 pengujian atau serangan yang diterapkan yaitu *Brute Force, MAC Address Spoofing, Sniffing to Evasdrop, Main in The Midele Attack,* dan *Ping Of Death.* Mungkin kedepanya mengunakan metode pungujian yang lain yang lebih efektif.