BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan yang sudah penulis lakukan dengan penelitian yang berjudul "Analisis Keamanan Jaringan (Wifi) Terhadap Serangan Packet Sniffing Dengan IDS", dengan menganalisis kedua *protocol* tersebut masih perlu adanya evaluasi dalam meningkatkan keamanan. Maka hasil penelitian ini dapat disimpulkan sebagai berikut :

1. Pada simulasi serangan *packet sniffing* terhadap *website HTTP dan HTTPS* kali ini penulis menggunakan jaringan *Wifi Indihome* dengan keamanan *WPA2-Personal*. Pada penyerangan *website HTTP tools ettercap* mampu merekam serta menampilkan *username* dan *password* dikarenakan tidak adanya enkripsi saat *web browser* dan *web server* melakukan komunikasi. Sedangkan pada *website HTTPS tools burpsuite* juga dapat merekam jejak dari aktivitas target saat mengakses *website* yang sudah terenkripsi dikarenakan *tools* ini memiliki hak istimewa karena memiliki sertifikat CA yang memungkinkan *tools* ini dapat melihat dan membaca pesan *request* dan *response* antara *web browser* dan *web server* yang terjadi dalam internet. Namun Jika memiliki keamanan yang lebih kuat seperti *facebook atau instagram* penyerang tidak dapat menampilkan *username* dan *password* dikarenakan adanya *enkripsi data SSL (Secure Socket Layer)* dan *TLS (Transport Layer Security)* yang memungkinkan *website* tersebut tidak dapat dibobol dengan mudah dan membutuhkan waktu yang cukup lama.
2. Pada simulasi serangan *Packet Sniffing* ini *tools Ettercap dan Burpsuite* dapat memonitoring hasil aktivitas pertukaran data yang lewat pada *web browser* dan *web server* dan dapat menampilkan *username* dan *password* saat melakukan autentifikasi login ketika penyerang dan target terhubung ke dalam satu jaringan (*Wifi*) yang sama.

5.2 Saran

Simulasi yang penyerang lakukan jauh lebih dari kata sempurna, masih banyak terdapat kekurangan. Maka dari itu dibutuhkan perkembangan lebih lanjut agar simulasi ini terlihat sempurna. Adapun saran dari simulasi ini sebagai berikut :

1. Simulasi ini akan lebih baik jika menggunakan 2 PC untuk melakukan serangan *packet sniffing*. Pada simulasi ini penulis hanya menggunakan 1 PC dalam melakukan pencurian data dan menggambarkan bagaimana serangan *packet sniffing* dapat terjadi.
2. Pada simulasi serangan *packet sniffing* ini penulis tidak mencoba menggunakan *device* lain sebagai target uji coba serangan *packet sniffing* dan hanya menggunakan satu *device* yang berfungsi sebagai penyerang dan target pada saat pengujian serangan *packet sniffing*.
3. Untuk dapat melakukan serangan *packet sniffing* menggunakan *tools ettercap dan wireshark* penulis harus terhubung pada jaringan *wifi* yang sama. Maka dari itu diperlukan keamanan terhadap jaringan *wifi* dengan menggunakan keamanan *WPA2-PSK*. Dengan ini dapat meminimalisir serangan *packet sniffing*. Sedangkan untuk serangan menggunakan *burpsuite* penyerang hanya perlu terhubung kedalam jaringan yang dapat mengakses internet dan menjalankan *burpsuite* untuk bertindak sebagai *proxy*.