BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring berjalannya waktu, perkembangan jaringan internet semakin meningkat pesat seiring meningkatnya jumlah *user* dan *endpoint device* yang membutuhkan layanan internet [1]. Hal ini menyebabkan meningkatnya jumlah perangkat *gateway* sebagai pintu masuk untuk mengakses jaringan internet. Tak terkecuali *gateway* pada jaringan WLAN yang menggunakan *Access Point* (AP). Jaringan WLAN menjadi jaringan yang banyak digunakan untuk terhubung dengan layanan internet baik secara privat maupun public [2]. Hal ini dikarenakan jaringan WLAN menggunakan gelombang radio untuk mentransmisikan data sehingga kecepatan transfer data cepat, praktis digunakan tanpa harus terhubung dengan kabel, dan fleksibel digunakan dalam posisi apapun selama *client* masih berada dalam cakupan gelombang radio dari AP. Namun karena transfer data yang bersifat terbuka menyebabkan data-data yang dikirimkan dalam proses transmisi dapat di-*capture* oleh siapapun sehingga jaringan WLAN sangat rentan terhadap pencurian data dan serangan *cyber*.

Serangan cyber pada jaringan WLAN yang sering terjadi berasal dari *client* atau *endpoint device* dalam cakupan gelombang radio AP. Biasanya penyerang melakukan monitoring terhadap paket-paket yang beredar pada gelombang radio AP untuk mencari informasi dan titik lemah dari AP untuk melakukan serangan terhadap jaringan ataupun *client* lain yang terhubung. Meskipun kini jaringan WLAN kebanyakan sudah memiliki sistem enkripsi yang mengubah paket data yang beredar pada gelombang radio AP menjadi *cypher text* dan mengharuskan *client* melakukan otentikasi *password* terlebih dahulu dengan AP. Serangan tidak dapat dihindarkan apabila penyerang memiliki *password* tersebut dan sistem enkripsi tersebut jarang digunakan pada jaringan WLAN publik. Sehingga untuk melindungi jaringan WLAN ini diperlukan sistem keamanan yang bisa mendeteksi serangan di titik AP yang berasal dari *client* sah maupun perangkat lain yang bukan *client*. Sistem keamanan yang cocok adalah *Wireless Intrusion*

Detection System (WIDS). WIDS adalah sistem keamanan WLAN yang dapat mendeteksi serangan-serangan yang dilancarkan dalam secara *wireless*. WIDS dapat dipasang dalam sensor terpisah dari AP atau dapat dijalankan dalam satu perangkat AP yang sama (hanya untuk perangkat yang mendukung).

Dalam tugas akhir ini, sistem keamanan WIDS dipasangkan pada jaringan WLAN yang dijalankan menggunakan *emulator* Mininet-Wifi. WIDS yang akan digunakan adalah WAIDPS (*Wireless* Auditing and IPS/IDS), yakni WIDS *open source* yang juga dapat digunakan untuk menguji serangan terhadap jaringan WLAN. Sistem jaringan ini diuji dengan serangan yang khusus ditujukan bagi jaringan WLAN untuk mengetahui kelayakan WIDS dalam mendeteksi serangan dan untuk mengetahui pengaruh pemasangan WIDS terhadap performa jaringan.

1.2 Rumusan Masalah

Rumusan Masalah dalam penelitian ini adalah:

1. Bagaimana menguji sistem keamanan WIDS pada jaringan WLAN agar dapat mengukur kelayakannya dalam mendteksi serangan dan mengetahui pengaruhnya terhadap performa jaringan secara akurat?
2. Bagaimana membangun sebuah sistem keamanan WIDS pada jaringan WLAN sehingga memiliki keamanan yang layak dan tidak menyebabkan penurunan performa jaringan?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1. Jaringan yang dibuat besifat *virtual*, hanya dijalankan menggunakan *emulator* yang dijalankan dalam laptop.
2. Perangkat *server* dan *switch* bersifat *virtual* sementara AP bersifat nyata karena dihubungkan dengan *physical* NIC melalui port pada laptop.
3. Sensor WIDS menggunakan USB *dongle* Wi-Fi yang dihubungkan pada laptop yang menjalankan jaringan virtual.
4. Perangkat penyerang berupa laptop kedua dan menggunakan perangkat Wi-Fi pada laptop tersebut untuk melakukan *monitoring* jaringan dan serangan *wireless*.

5. Pada uji serangan *evil-twin*, digunakan USB *dongle* Wi-Fi kedua yang dihubungkan pada laptop penyerang untuk keperluan serangan.
6. Perangkat *client* sah (bukan penyerang) berupa *smartphone*. Jumlah *client* sah hanya berjumlah 1 karena keterbatasan alat.
7. Emulator jaringan yang digunakan adalah Mininet-WiFi.
8. WIDS yang digunakan adalah WAIDPS.
9. Pengujian yang dilakukan menggunakan serangan WEP.WPA, dan WPA2 *cracking*; *deauthentication denial of service*; dan *evil-twin*.
10. QoS yang diukur adalah *delay, jitter, throughput*, dan *packet loss*.
11. Proses *handoff* tidak diperhatikan.

1.4 Tujuan dan Manfaat

1.5. 1 Tujuan

Tujuan dari penelitian tugas akhir ini adalah :

1. Menguji sistem keamanan WIDS pada jaringan WLAN dengan serangan yang khusus ditujukan bagi jaringan WLAN untuk mengetahui tingkat kelayakan keamanan WIDS dan pengaruh pemasangan WIDS pada performa jaringan.

1.5. 2 Manfaat

Manfaat dari penelitian tugas akhir ini adalah :

1. Sistem jaringan dapat diterapkan untuk mengelola jaringan WLAN secara aman di area kampus atau untuk jaringan di rumah sendiri.
2. Sistem jaringan yang dibuat nantinya bisa menjadi sarana pembelajaran dan demonstrasi tentang keamanan WIDS pada jaringan WLAN.

1.5 Metode Penelitian

Metodologi penelitian yang digunakan dalam menyelesaikan tugas akhir ini adalah sebagai berikut:

1. Studi Literatur

   Tahap ini berisi kegiatan pengumpulan dan pembelajaran terhadap referensi berupa artikel, jurnal, ataupun buku yang berhubungan dengan penelitian.

2. Perancangan Sistem

Tahap ini berisi kegiatan perancangan sistem jaringan yang akan dibuat. Perancangan sistem dibuat berdasarkan perangkat apa saja yang dibutuhkan dalam jaringan dan bagaimana mereka berkomunikasi.

3. Implementasi Sistem

Tahap ini berisi kegiatan implementasi sistem pada software dan hardware yang telah dikonfigurasi terlebih dahulu. Pada tahap ini juga dilakukan uji coba kompatibilitas dan stabilitas software dan hardware yang digunakan.

4. Pengujian dan Analisis Hasil Sistem

Tahap ini berisi kegiatan pengujian sistem terhadap skenario yang telah ditentukan. Setelah itu dilakukan dokumentasi dan pengambilan data-data hasil pengujian untuk dilakukan analisis apakah sistem yang telah dibangun sudah memenuhi kelayakan atau tidak. Jika tidak layak maka akan dicari faktor yang menyebabkan ketidak-layakan.

5. Penyusunan Laporan Akhir

Tahap ini berisi kegiatan penyusunan laporan yang berisi hasil penelitian yang dilakukan dari awal hingga mendapat hasil akhir.

1.6 Sistematika Penulisan

Sistematika penulisan dari Tugas Akhir ini dibagi menjadi lima bab dengan masing-masing bab berisi sebagai berikut:

BAB I PENDAHULUAN

Pada BAB I ini dijelaskan mengenai latar belakang, penelitian terkait, rumusan masalah, batasan masalah, tujuan dan manfaat, metode penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada BAB II diuraikan mengenai dasar teori dan penjelasan yang mendukung penulisan Tugas Akhir ini.

BAB III PERANCANGAN SISTEM

BAB III menjelaskan mengenai perancangan dari sistem yang digunakan dan scenario yang dilakukan untuk menguji sistem dalam Tugas Akhir ini. Dijelaskan bagaimana skenario perancangan dari jaringan WLAN yang dilengkapi sistem keamanan WIDS dan scenario apa saja yang diujikan pada jaringan tersebut.

BAB IV PENGUJIAN SISTEM DAN ANALISIS

Pada BAB IV membahas dan menjelaskan hasil dari pengujian sistem.

BAB V KESIMPULAN DAN SARAN

BAB ini menjelaskan kesimpulan dari masalah yang telah dijelaskan pada penelitian Tugas Akhir ini. Serta berisi saran dari Tugas Akhir ini yang dapat menunjang untuk penelitian berikutnya sebagai bahan referensi.