BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi *wireless* saat ini berkembang sangat pesat. Karena kemudahan dan penggunaannya yang dapat dilakukan dimana saja, menyebabkan teknologi *wireless* rentan terhadap serangan dari pihak yang tidak bertanggung jawab. Penyadapan pada jalur komunikasi dapat dilakukan lebih mudah karena tidak perlu mencari jalur kabel untuk melakukan hubungan. Hal tersebut menyebabkan sistem yang tidak menggunakan sistem keamanan ataupun enkripsi akan mudah ditangkap.

Terdapat banyak ancaman keamanan dan serangan yang dapat mengganggu komunikasi didalam jaringan, salah satunya adalah *Man in The Middle* (MitM) *Attack* dengan teknik serangan ARP *poisoning*. ARP poisoning lebih mudah diatasi pada *guided media* (*wire connection*), karena semua komunikasi dibatasi oleh sebuah *physical link* di antara *workstation*. Namun berbeda dengan *unguided media* (*wireless connection*) yang menggunakan frekuensi radio sebagai jalur komunikasinya, serangan tersebut akan lebih sulit diatasi. Metode serangan ARP *poisoning* sangat merugikan bagi *user* karena bersifat aktif, yaitu penyerang dapat melakukan tindakan langsung pada *user*, contohnya mencuri *username* dan *password* dari korban yang dituju. Mengingat aktifitas yang sering dilakukan ketika terhubung dengan jaringan internet seperti membuka E-mail, browsing dan melakukan transaksi internet banking. Serangan tersebut akan sangat merugikan bagi *user*.

Ada beberapa solusi untuk mengatasi serangan dari MitM *attack* dengan teknik ARP *spoofing* tersebut seperti *static* ARP *table,* metode ini bekerja dengan cara mendaftarkan setiap *user* yang terkoneksi di jaringan secara manual kedalam cache table. Namun metode ini masih memiliki kekurangan yaitu admin tidak dapat mendaftarkan semua *user* yang akan terkoneksi ke jaringan WLAN (*wireless* LAN). Oleh karena itu dibutuhkan cara yang lebih efektif dari segi

efisiensi waktu dan biaya. Maka untuk mengatasi masalah tersebut dapat ditanggulangi dengan menggunakan metode *isolation user*, pada metode ini setiap *user* ditempatkan pada *pool* DHCP yang berbeda-beda agar *intruder* tidak dapat melakukan *poisoning* pada *user* lain yang terhubung ke jaringan. Metode ini memanfaatkan DHCP *server* yang memberikan IP *address* dengan prefix /30.

Harapan dari penelitian ini adalah agar sistem keamanan yang dibuat dapat diterapkan pada lingkungan publik yang menyediakan layanan *wireless* seperti: perhotelan, akademik, kafe dan tempat publik lainnya dan juga dapat membuat layanan yang aman bagi para pengguna jaringan *wireless* dari serangan ARP *poisoning*.

1.2 Rumusan Masalah

Dari latar belakang tersebut, maka timbul permasalahan yaitu:

1. Bagaimana serangan dari ARP *poisoning.*
2. Bagaimana membangun sistem keamanan pada jaringan *wireless* untuk mencegah serangan ARP *poisoning.*
3. Bagaimana kelemahan dan kelebihan dari metode *isolation user.*

1.3 Maksud dan Tujuan

Adapun maksud yang hendak dicapai adalah :

1. Mencegah terjadinya serangan dari ARP *poisoning*.
2. Memastikan *traffic user* yang terhubung dalam jaringan *wireless* tidak dapat di*sniffing* oleh pihak yang tidak bertanggung jawab.

Adapun tujuan yang ingin dicapai dengan adanya alat tersebut, yaitu :

1. Menganalisa ARP *poisoning* didalam jaringan *wireless.*
2. Mengimplementasikan sistem keamanan jaringan *wireless* menggunakan metode *isolation user*.
3. Menganalisa serangan menggunakan wireshark.
4. Menganalisa kelebihan dan kekurangan dari metode *isolation user.*

1.4 Batasan Masalah

Masalah yang akan dikaji dan dibahas meliputi :

1. Menggunakan metode *isolation user*.
2. Menggunakan prefix /30.
3. Hardware yang digunakan adalah Mikrotik RB750
4. Access point Linksys Cisco WAG120N.
5. Serangan ARP *poisoning* menggunakan aplikasi Cain & Abel dan Ettercap.
6. Analisa serangan dengan wireshark.
7. Pengujian pada penelitian ini akan dilakukan pada situs HTTP.

1.5 Metodologi

Dalam melakukan penelitian ini, akan digunakan beberapa tahap dalam menyelesaikan penelitian, diantaranya adalah:

1. Studi literatur

Pada tahap ini dilakukan pengumpulan literatur mengenai teknik serangan MitM serta metode *isolation user* yang merupakan salah satu metode yang digunakan untuk mencegah serangan tersebut, baik berupa buku keamanan jaringan, jurnal maupun artikel di internet.

2. Analisa kebutuhan

Pada tahap ini menentukan beberapa kebutuhan yang diperlukan oleh sistem keamanan jaringan *wireless* baik *software* ataupun *hardware.* Tahap ini juga dilakukan berdasarkan beberapa literatur yang sudah didapat.

3. Rancangan sistem

Tahap rancangan sistem merupakan tahapan yang dilakukan untuk merancang topologi yang sesuai untuk membangun sistem.

4. Implementasi

Pada tahap ini dilakukan implementasi dari sistem berdasarkan rancangan yang sudah dibuat. Proses pencegahan serangan dilakukan melalui konfigurasi *router* mikrotik, sedangkan teknik serangan dilakukan menggunakan aplikasi *Cain & Abel*.

5. Pengujian dan analisa hasil

Pada tahap ini, dilakukan pengujian secara fungsional serta analisa terhadap hasil dari sistem yang dibuat. Pengujian dilakukan dengan cara melakukan serangan terhadap sistem sebelum ditambahkan pengamanan dan terhadap sistem setelah ditembahkan pengamanan. Analisa dilakukan untuk mengetahui semua kemungkinan serangan yang dapat terjadi pada sistem yang telah dibuat.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakang, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian dan sistematika penulisan.

BAB II TEORI PENUNJANG

Bab ini menjelaskan dan menguraikan teori penunjang yang dibutuhkan dalam tugas akhir, yaitu teori tentang Media transmisi, Arsitektur jaringan, Internet protokol, Jaringan *wireless*, keamanan jaringan, dan metodologi desain jaringan.

BAB III PERANCANGAN SISTEM

Bab ini menjelaskan tentang perancangan sistem yang dibangun berdasarkan pada metodologi desain jaringan, meliputi tahap persiapan (*prepare*), tahap perencanaan (*plan*), tahap desain (*design*), tahap implementasi (*implementation*), tahap operasi (*operate*), tahap optimalisasi (*optimize*).

BAB IV HASIL PENGUJIAN DAN ANALISA

Bab ini menjelaskan tentang pengujian dan analisa sistem, meliputi pengujian dan analisa terhadap hasil perancangan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran dari seluruh pembahasan materi.