BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Jaringan komputer merupakan teknologi yang sangat berkembang saat ini. Seiring berkembangnya teknologi jaringan komputer, serangan yang memanfaatkan celah – celah keamanan pada jaringan komputer juga semakin meningkat.

Salah satu serangan yang sering terjadi adalah *Address Resource Protocol* (ARP) *spoofing*, dimana penyerang mengirim ARP *message* palsu ke jaringan lokal. Tujuan penyerangan ini ialah agar *Media Access Control* (MAC) *address* penyerang diasosiasikan dengan *Internet Protocol* (IP) *address* dari *host* lain (biasanya *default gateway*), sehingga seluruh koneksi ke IP *address* tersebut dialihkan ke penyerang. Biasanya serangan ini digunakan sebagai pembuka untuk serangan-serangan lain, seperti *Denial of Service* (DoS), *Man in the Middle* (MiM), atau *session hijacking*[1].

Saat ini, penanganan serangan ARP *spoofing* di jaringan komputer sudah diimplementasikan oleh aplikasi – aplikasi di *Personal Computer* (PC), baik *desktop* maupun *laptop*. Beberapa pendeteksian ARP *spoofing* sudah cukup banyak diimplementasikan dengan menginstall aplikasi – aplikasi pendeteksi ARP *spoofing* pada komputer.

Namun beberapa jenis penanganan tersebut hanya terjadi di sisi pengguna yang menggunakan aplikasi pelindung di dalam jaringan tersebut, dapat memperlambat ARP, atau terlalu kompleks untuk diterapkan[2]. Untuk menciptakan jaringan yang lebih aman, terutama di tempat umum, dimana tidak semua pengguna

menggunakan aplikasi pelindung sebaiknya serangan dapat dicegah sebelum *host victim* terkena serangan dan salah satu caranya yaitu saat paket serangan mencapai *switch* atau *access point*[2]. Namun bentuk – bentuk pencegahan ini masih terbatas pada jaringan static, memerlukan pergantian terhadap seluruh host di jaringan, atau memerlukan *switch* yang terlalu mahal[2].

Untuk mengatasi batasan – batasan sumber daya tersebut, dapat digunakan OpenFlow *switch* yang menyediakan sebuah protokol terbuka untuk memprogram *flow-table* pada *switch* dan *router* yang berbeda[3]. Beberapa kelebihan yang dimiliki oleh OpenFlow *switch* seperti berikut:

- *Controller* jaringan yang aman dan mudah diatur untuk mengontrol *flow*
- Memiliki performa tinggi dan implementasi yang terjangkau
- Pemisahan eksperimental *traffic* dan *production traffic* yang dapat dipastikan
- Lebih mudah untuk mengantisipasi serangan yaitu dengan cara memblokir *port* yang terhubung ke penyerang
- Memiliki fitur – fitur tambahan yang tidak dimiliki *switch* biasa seperti mengenerate ping dan ARP

Berdasarkan latar belakang tersebut penelitian ini membahas dan mengusulkan sebuah *network-based intrusion prevention system* dengan *stateful protocol analysis* sebagai teknik pendeteksian yang digunakan untuk mendeteksi dan mencegah ARP *spoofing* dalam pengimplementasian *intrusion prevention system* pada jaringan OpenFlow *switch*.

1.2. Rumusan Masalah

Berdasarkan masalah yang diuraikan di atas maka pokok permasalahan yang dikaji dalam penelitian ini dirumuskan sebagai berikut: “Bagaimana mendeteksi dan mencegah serangan ARP *spoofing* pada LAN menggunakan OpenFlow *switch*?”

1.3. Batasan Masalah

Batasan-batasan dan ruang lingkup penelitian ini:

a. Penelitian dilakukan pada jaringan *virtual* menggunakan aplikasi Mininet pada sistem operasi Linux.
b. *Controller* OpenFlow yang digunakan adalah POX *controller*.
c. Penelitian menggunakan OpenFlow *switch* sebagai *switch* yang digunakan.

1.4. Tujuan Penelitian

Berikut beberapa tujuan dari penelitian ini:

a. Mencegah terjadinya serangan ARP *spoofing* pada LAN untuk menjamin keamanan jaringan lokal.
b. Mengusulkan mekanisme pendeteksian dan pencegahan ARP *spoofing* yang diimplementasikan dalam sebuah OpenFlow *controller*.

1.5. Manfaat Penelitian

Hasil penelitian ini diharapkan dapat bermanfaat secara akademis dan secara praktis.

1.5.1. Manfaat Akademis

Manfaat yang dapat diperoleh dari penelitian ini secara akademis adalah sebagai bahan masukan bagi penelitian yang serupa atau penelitian yang sifatnya lebih luas di masa yang akan datang.

1.5.2. Manfaat Praktis

Manfaat yang dapat diperoleh dari penelitian ini secara praktis adalah OpenFlow *controller* yang dibuat dapat diimplementasikan sebagai keamanan jaringan lokal terhadap serangan ARP *spoofing*.