BAB I
PENDAHULUAN

1.1. Latar Belakang

Internet merupakan sebuah keniscayaan yang melatarbelakangi terciptanya era keterbukaan informasi. Manfaat utama dari penggunaan internet adalah untuk bertukar informasi sesama pengguna. Manfaat ini dapat dirasakan karena adanya infrastruktur pendukung yang memadai. Infrastruktur jaringan internet yang menghubungkan antara *Internet Service Provider* (ISP) dengan pengguna merupakan komponen utama dari fasilitas penunjang pemanfaatan internet.

Terdapat banyak komponen di dalam sebuah jaringan komunikasi internet seperti protokol komunikasi, perangkat keras jaringan, dan perangkat lunak pendukung lainnya. Masing-masing dari komponen tersebut memiliki peran vital dalam proses pengiriman data melalui jaringan. Protokol komunikasi adalah komponen yang berperan mengatur bagaimana komunikasi antar perangkat dapat dilakukan.

Data yang dikirim melalui jaringan memiliki potensi dicuri atau dirusak dengan sengaja oleh pihak-pihak yang tidak bertanggungjawab. Salah satu cara yang digunakan untuk melakukan hal tersebut adalah dengan mengeksploitasi kerentanan yang ada pada protokol komunikasi jaringan. *Address Resolution Protocol* (ARP) adalah protokol yang sangat rentan untuk dieksploitasi khususnya pada jaringan WLAN (*Wireless Local Area Network*). Eksploitasi dari protokol ini biasa disebut ARP *Spoofing* atau ARP *Poisoning*. Contoh serangan yang memanfaatkan eksploitasi dari protokol tersebut antara lain *Man in The Middle Attack* (MiTM), DNS *Spoofing, Netcut,* dan lain-lain. Untuk itu, perlu ada mekanisme pengamanan guna memperkecil resiko terjadinya ekspoitasi protokol komunikasi dalam jaringan.

Sampai saat ini, eksplotasi dari protokol *address resolution protocol* masih sering terjadi. Pada tempat-tempat umum seperti kampus, perkantoran, dan instansi-instasi khusus pemerintah yang memberikan akses WIFI gratis sering sekali terjadi penyalahgunaan dari protokol ARP. Hal tersebut didukung oleh laporan Owasp Mobile Top 10 pada tahun 2016. Penyerang umumnya menyalahgunakan serangan ARP *spoofing* untuk menegahi koneksi antara pengguna jaringan dan *access point* untuk membaca paket yang dikirimkan penggu na ke internet.

Jaringan WLAN merupakan jaringan berskala kecil yang digunakan di area perkantoran, kampus, dan instansi-instansi pemerintah sebagai sarana pengaksesan internet. Jaringan di tempat-tempat tersebut umumnya merupakan jaringan terbuka yang dapat diakses oleh semua orang tanpa ada otentikasi *password*. Hal ini menjadikan jaringan pada area tersebut sangat rentan untuk dieksploitasi salah satunya menggunakan ARP *spoofing*, meskipun tidak semua jaringan tersebut terbuka, tetap saja ada resiko jaringan tersebut untuk dieksploitasi. Dengan menggunakan teknik tersebut, data-data pribadi pengguna jaringan akan dapat diambil oleh pihak-pihak yang tidak bertanggungjawab.

Berdasarkan latar belakang di atas, penulis berusaha membuat sebuah *security control* berupa program yang dapat mendeteksi, memitigasi, serta mengamankan pengguna jaringan WLAN di area tersebut dari serangan yang memanfaatkan ekspoitasi *address resolution protocol* (ARP). Program ini membandingkan antara MAC *address* dari *router* asli, yang disimpan pada sebuah variabel secara statis, dengan MAC *address* dari *router* yang disimpan secara dinamis pada ARP *cache table*. Jika MAC *address* yang dibandingkan tidak cocok, maka dapat dinyatakan bahwa ada serangan ARP *spoofing* pada jaringan tersebut. Program kemudian akan mengeluarkan perangkat penyerang dari jaringan, berdasarkan MAC *address* yang didapat dari ARP *cache table,* menggunakan *deauthentication attack*. Oleh karena itu, penulis memberi judul pada penelitian ini, ” **Pengamanan *Wireless Local Area Network* dari Serangan**

***Address Resolution Protocol Spoofing* Menggunakan Pendekatan Deteksi Pasif dan *Deauthentication Attack* Berbasis Raspberry Pi**".

1.2. Rumusan Masalah

Berdasarkan pemaparan latar belakang di atas, dapat disimpulkan bahwa terdapat rumusan masalah:

- Apakah deteksi pasif dan *deauthentication attack* efektif untuk mengamankan jaringan WLAN dari serangan ARP *spoofing*?
- Seberapa cepat waktu yang dibutuhkan sistem untuk mendeteksi dan merespon serangan ARP *Spoofing* pada jaringan WLAN menggunakan deteksi pasif dan *deauthentication attack*?

1.3. Tujuan Penelitian

Tujuan penilitian berdasarkan pemaparan latar belakang dan rumusan masalah dalam hal ini adalah mengamankan jaringan WLAN dari serangan ARP *spoofing.*

1.4. Manfaat

Berdasarkan latar belakang, rumusan masalah, dan tujuan penelitian yang telah dipaparkan di atas, dapat disimpulkan bahwa penilitian ini memiliki manfaat:

- Dapat menjadikan luaran yang diharapkan dari penelitian ini sebagai *security control* untuk memitigasi resiko terhadap serangan ARP *spoofing*.
- Dapat dijadikan referensi untuk penelitian yang terkait dengan pembahasan pada tulisan ini.

1.5. Ruang Lingkup

Ruang lingkup dari pembahasan pada penelitian ini:

- Sistem pengamanan bekerja pada jaringan WLAN.
- Penelitian membahas cara melindungi jaringan WLAN dari serangan ARP *spoofing.*

- Penelitian ini berfokus untuk membahas cara melindungi jaringan dari serangan ARP *spoofing* yang mentargetkan seluruh perangkat yang ada di jaringan.

1.6 Luaran Yang Diharapkan

Luaran yang diharapkan pada penelitian ini adalah sebuah program yang dapat digunakan oleh *network administrator* sebagai *security control* untuk mengamankan jaringan WLAN dari serangan ARP *spoofing*.

1.7 Sistematika Penulisan

Penulis akan memaparkan gambaran sistematika penulisan laporan penelitian ini yang terdiri dari beberapa bagian utama berikut:

BAB 1 Pendahuluan

Bab ini membahas mengenai latar belakangan, rumusan masalah, tujuan, manfaat, ruang lingkup, dan luaran yang diharapkan dari penelitan.

BAB 2 Landasan Teori

Bab ini membahas tentang teori-teori berdasarkan referensi terkait dengan pembahasan pada penelitian ini.

BAB 3 Metodologi Penelitian

Bab ini membahas metode, kerangka berfikir, dan jadwal kegiatan yang dilakukan dalam penelitian.

BAB 4 Hasil dan Pembahasan

Bab ini membahas hasil dan analisis dari penelitian yang dilakukan pada skripsi ini

BAB 5 Penutup

Bab ini membahas kesimpulan dan saran dari penelitian ini.

Daftar Pustaka

Lampiran