BAB I

PENDAHULUAN

1.1 Latar Belakang

Dari waktu ke waktu, kemajuan teknologi terus berkembang. Hal tersebut terjadi untuk memenuhi kebutuhan manusia agar dalam menjalankan aktivitasnya dimudahkan. Salah satu dari perkembangannya adalah jaringan komputer. Jaringan komputer merupakan sebuah sistem yang terdiri dari komputer, *software*, dan perangkat-perangkat lainnya yang bekerja sama agar bisa berkomunikasi dengan membagi sumber daya serta pengaksesan informasi [1]. Namun, dibalik dari kemudahan yang disediakan oleh jaringan komputer tersebut terdapat sangat banyak ancaman kejahatan atau resiko pada bidang ini atau yang biasa disebut dengan *cyber crime* [2]. Ancamannya dapat berupa baik fisik maupun logik yang secara langsung maupun tidak langsung mengganggu kegiatan yang sedang berlangsung pada jaringan. Banyak faktor penyebab resiko dalam jaringan komputer yang diantaranya dijelaskan pada bab landasan teori.

Salah satu jenis *cyber crime* yang bisa terjadi yaitu dengan teknik ARP *spoofing* dimana ancaman tersebutlah yang dijadikan fokus pada penelitian kali ini. *Spoofing* sendiri artinya adalah menjelma atau menyamar. Di lain hal, ARP atau *Address Resolution Protocol* merupaka protokol yang bertugas

untuk meresolusi alamat IP ke alamat fisik (*MAC address*). Terdapat dua elemen utama pada ARP ini yaitu paket *request* dan paket *reply*. Paket *request* dikirim secara *broadcast* yang berisikan "Siapa yang memiliki IP *address* sekian?". *Host* yang bersangkutan menjawab secara *unicast* yang berisi "Saya yang punya IP *address* sekian, MAC *address* saya sekian". Dengan kata lain, teknik ARP *spoofing* merupakan teknik yang digunakan penyerang dengan memalsukan alamat IP menjadi IP korban sehingga penyerang bisa mendapatkan data-data yang dikirim dan diterima korban, tanpa diketahui oleh korban.

Terdapat beberapa hasil penelitian berupa metode/teknik yang dikembangkan untuk mengatasi serangan ARP *spoofing*. Diantaranya adalah *Guarding Algorithm* [3], *Man-In-The-Middle Defiant* (MD-ARP) dan *voting* [4], *Effective and Secure* ARP (ES-ARP) [5], *Bandwidth Management* [1]. Masing-masing metode memiliki kelebihan dan kelemahan.

Guarding Algorithm [3] mengajukan metode yang membatasi modifikasi ARP *cache*. Metode ES-ARP [5] bekerja dengan mem-*broadcast* paket ARP *request* dan *reply*. Namun, perbedaan dengan ARP normal adalah ES-ARP akan meng-*update* ARP *cache*-nya setiap kali menerima ARP *request* dan ARP *reply* dari *host* manapun dalam satu jaringan. Jika entri pemetaan IP-MAC yang didapat sama dengan yang sudah ada dalam ARP *cache*-nya, paket ARP tersebut akan dibuang. Menurut penelitiannya, cara ini

terbukti bahwa jumlah *traffic* komunikasi lebih efisien dan aman dibandingkan dengan metode lainnya. Tetapi, ES-ARP belum memperhatikan validasi paket yang datang. Oleh karena itu, metode ini hanya mengasumsikan penyerang datang setelah jaringan tersebut telah memiliki pemetaan IP-MAC *host* yang otentik. Jika penyerang mampu lebih dulu menyebarluaskan *mapping* yang palsu, maka satu jaringan akan terkena ARP *spoofing*.

Sementara itu, metode MD-ARP [4] menerapkan dua metode yang berbeda, yaitu MD-ARP sendiri dan *voting* [4]. MD-ARP memiliki dua tabel yang mendukung pemetaan. Tabel tersebut yaitu *long term* dan *short term*. MD-ARP akan mengirimkan 50 paket ARP *request*. Jika setidaknya terdapat 1 paket *reply*, maka *mapping* tersebut akan diregistrasi. Sedangkan *voting* akan berlaku jika terdapat *host* baru pada suatu jaringan. *Voting* bekerja dengan cara menanyakan *mapping* IP-MAC tertentu ke *host* "tetangga". Hasil *polling* akan dikalkulasi oleh *host* penanya. Jika terdapat lebih dari 50% respon *mapping* yang sama dari yang bersangkutan, maka *mapping* itulah yang dianggap sebagai *mapping* asli. Selain itu, *voting* berlaku jika terdapat IP *conflict*. Namun, jika *voting* diberlakukan secara terus-menerus, *traffic* akan ramai dan rentan terhadap ancaman *Denial of Service* (DoS) karena *host* yang ditanya akan mengirimkan 50 paket ARP *voting reply*. Kedua metode ini jika digabungkan akan memenuhi *traffic* komunikasi dan dapat menyebabkan

router tidak dapat bekerja secara maksimal terutama *router* berspesifikasi rendah.

Dari permasalahan yang timbul, terdapat ide bagi penulis untuk melakukan penelitian mengenai pencegahan ARP *spoofing* yang didasari pada penelitian-penelitian sebelumnya. Adanya kekurangan dan kelebihan masing-masing kedua metode membuka peluang bagi penulis untuk menentukan metode yang akan diteliti. Metode tersebut yaitu ES-ARP berbasiskan *voting* atau yang kemudian disebut sebagai ESV-ARP. *Voting* akan diberlakukan tiap kali ada *IP conflict* dan mengirimkan paket *voting* secara *broadcast* layaknya metode ES-ARP.

1.2 Rumusan Masalah

Masalah penelitian dirumuskan sebagai berikut: "Bagaimana cara untuk mencegah agar komputer *client* terhindar dari serangan ARP *spoofing* dengan metode ES-ARP berbasis *voting* yang efektif dan efisien?"

1.3 Batasan Masalah

Penelitian berpusat pada implementasi deteksi dan pencegahan ARP *spoofing*. Adapun pembatasan masalah pada penelitian kali ini sebagai berikut:

1. Teknik yang digunakan adalah ES-ARP berbasis *voting* (ESV-ARP).

2. *Spoofing* dilakukan pada jaringan lokal atau *Local Area Network* (LAN).
3. Penelitian terletak pada level aplikasi pada model OSI.
4. Bahasa pemrograman yang digunakan pada pembuatan aplikasi adalah C# dengan media Visual Studio 2010 Professional.
5. Tidak dilakukan enkripsi paket ARP.
6. Pengujian dilakukan dengan menggunakan 3 komputer virtual pada VirtualBox dengan sistem operasi Windows 7.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk menjawab rumusan masalah dengan mengimplementasikan metode yang efektif untuk melindungi komputer *client* dari serangan ARP *spoofing* disertai dengan pembuatan program aplikasi berupa Windows *Form*.

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat digunakan sebagai fasilitas untuk membangun keamanan dalam jaringan komputer sehingga dapat memberikan rasa aman dan nyaman bagi pengguna dari serangan ARP *spoofing*.

1.6 Sistematika Penulisan

Penulisan skripsi ini menggunakan sistematika penulisan sebagai berikut:

- BAB I: PENDAHULUAN

  Bab pendahuluan terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat peneletian, dan sistematika penulisan.

- BAB II: LANDASAN TEORI

  Bab landasan teori menguraikan teori-teori yang berkaitan mengenai penelitian dan metode-metode yang telah digunakan sebelumnya sebagai referensi penelitian.

- BAB III: METODOLOGI PENELITIAN

  Bab ini menggambarkan penerapan penggabungan metode algoritma ES-ARP dan *voting*, perancangan dan implementasi *interface* aplikasi yang disertai dengan *flowchart* sehingga menjadi produk program aplikasi yang kemudian dapat digunakan oleh *client*.

- BAB IV: ANALISIS DAN PEMBAHASAN

  Bab ini memaparkan hasil pengujian yang dilakukan terhadap aplikasi beserta dengan pembahasan dan penjelasan terhadap hasil yang dicapai.

- BAB V: KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan dan jawaban atas rumusan masalah penelitian serta saran berdasarkan hasil uji coba yang didapat.