BAB I
PENDAHULUAN

1.1 Latar Belakang

Dewasa ini perkembangan zaman menyebabkan Jaringan komputer semakin berkembang pesat sehingga tuntutan masyarakat akan kebutuhan jaringan semakin beragam. Pengguna atau komunitas itu sendiri dapat mengakses informasi publik dan pribadi. Internet merupakan salah satu sarana pengumpulan informasi, berbagai informasi tersebut dapat diperoleh melalui dunia maya. Sebelum berkembang, akses untuk mendapatkan informasi belum semudah saat ini. Informasi hanya tersedia pada surat kabar yang diantar tukang surat atau pada saat membeli dipenjual surat kabar, tetapi sekarang perkembangan untuk mendapatkan informasi dapat dengan mudah didapatkan hanya dengan menghubungkan ke jaringan internet (YUDIANTO, M. Jafar Noor; NOOR, Jafar 2014).

Masalah keamanan Jaringan komputer merupakan hal yang sangat penting dan perlu diperhatikan dalam pengembangan Jaringan komputer. Jaringan yang terhubung ke perangkat jaringan biasanya rentan terhadap peretasan atau *hacking*. Peretasan merupakan suatu kegiatan yang memungkinkan seseorang atau kelompok untuk mengubah atau mengambil data untuk kepentingan pribadi. Contohnya seperti *phissing* dimana terdapat informasi berupa *username, password* atau informasi pribadi lainnya yang dapat disalahgunakan dan menyebabkan kerugian bagi pihak lain. Hal tersebut terjadi ketika perangkat jaringan diberikan akses untuk menggunakan jaringan. Saat membangun sistem keamanan jaringan, perlu lebih memperhatikan perlindungan sumber daya yang tersimpan di jaringan agar meminimalisir adanya kebocoran data, terutama jaringan perusahaan atau pemerintah yang menyimpan banyak data penting (ENGEBRETSON, Patrick, 2013).

Address Resolution Protocol (ARP) Poisoning merupakan Teknik yang digunakan untuk menyerang sebuah jaringan, teknik ini memanipulasi tabel *ARP* dengan cara mengirimkan paket *ARP* palsu ke dalam jaringan sehingga tabel *ARP* yang asli akan tertimpa dengan tabel *ARP* palsu yang dikirim penyerang. *Address*

Resolution Protocol (ARP) merupakan protokol dalam *TCP/IP Protocol Suite* yang bekerja diantara *network layer* dan *data link layer* dan bertanggungjawab dalam melakukan resolusi pencatatan dan pencocokan alamat IP ke dalam alamat *Media Access Control* (*MAC* Address) lalu hasilnya letakkan didalam *ARP cache* (Kamajaya et al., 2020).

Jaringan *client server* diartikan sebagai suatu perancangan Jaringan komputer yang mana perangkat *client* melakukan proses meminta data, dan *server* yang bertugas untuk memberikan respon dari *feedback* yang berupa data. *Client* adalah individu yang terhubung ke server untuk meminta data atau layanan dari server sementara server adalah individu yang menyediakan data atau layanan yang diharapkan oleh klien (Refflan, 2012).

Client-Server adalah pembagian kerja antara server dan klien memiliki akses ke *server* pada jaringan. Dengan demikian, arsitektur *client-server* merupakan desain aplikasi yang berisi *client* dan *server* yang saling berkomunikasi ketika ingin mengakses *server* untuk suatu jaringan. Klien juga sering menginginkan akses penuh ke router, sehingga klien dapat mendapatkan akses informasi yang berada dipusat yaitu di router. Namun dengan menambah jumlah router yang banyak maka akan menimbulkan biaya yang relatif besar. Router sangat berguna untuk mendistribusikan IP address dengan baik. Terdapat juga penelitian dengan forensik jaringan yang dapat merekam kejadian atau aktifitas lalu lintas data pada sebuah jaringan. Setelah diinvestigasi dan dilakukan analisa diduga dapat ditemukan bukti aliran paket yang mencurigakan, hal tersebut bertujuan untuk menemukan IP address penyusup (Hafizh et al., 2020). Setelah ditemukannya serangan maka diperlukan pengambilan keputusan terhadap ancaman yang terjadi, diharapkan terdapat rekomendasi *tools* yang berfungsi untuk mendeteksi dan mengidentifikasi serangan serta menangani dan upaya pencegahan serangan ARP (Forensik Metarouter pada Lalu Lintas Jaringan Klien Firmansyah et al., 2019).

Berdasarkan latar belakang dan fenomena tersebut, maka diangkat sebuah judul yaitu analisis transfer data pada jaringan terdampak *ARP Spoofing* menggunakan *ARP Poisoning* dan statistik deskriptif. Pada penelitian ini digunakan router 2800 yang berada di Laboratorium Jaringan komputer Institut Teknologi

Dirgantara Adisutjipto (ITDA). Dengan adanya analisis mengenai jaringan yang terkena *ARP Poisoning*, maka praktisi dan administrator dapat memberikan pencegahan ketika perangkat jaringan terkena *ARP Poisoning*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, dapat dirumuskan beberapa masalah sebagai berikut :

1. Bagaimana pengaruh *ARP Poisoning* ketika transfer data pada Router Cisco 2800 dalam sebuah jaringan?
2. Bagaimana melakukan tindakan pencegahan terhadap Jaringan komputer saat melakukan transfer data terhindar dari serangan *ARP Poisoning*?

1.3 Batasan Masalah

Pembatasan masalah tujuannya untuk menghindari penyimpangan atau pelebaran pokok pembahasan dalam mencapai tujuan penelitian. Berdasarkan rumusan masalah yang telah disebutkan, maka didapatkan batasan masalah sebagai berikut :

1. Perangkat yang diuji adalah perangkat jaringan intra yang berada di laboratorium komputer ITDA Yogyakarta.
2. Perangkat yang digunakan adalah 20 buah personal komputer, satu buah laptop, dua buah switch, satu buah Router Cisco 2800.
3. Pengujian dilakukan menggunakan Distro Linux Kali Linux sebagai media untuk melakukan proses penyerangan terhadap target di Laboratorium Komputer ITDA.
4. Hasil analisis hanya pada penyerangan menggunakan *ARP Poisioning Attack* yang dilakukan menggunkan Kali Linux.

1.4 Tujuan Penelitian

Penelitian dengan judul analisis transfer data pada jaringan terdampak *ARP Spoofing* menggunakan metode *ARP Poisoning* dan statistik deskriptif ini mempunyai tujuan:

1. Mengetahui pengaruh *ARP Spoofing* ketika transfer data pada router dilakukan.

2. Menjabarkan celah keamanan serta mengukur tingkat keamanan yang perlu untuk segera diperbaiki sehingga dapat membantu untuk memperbaiki kegagalan dalam mempertahankan keamanan sistem informasi dan jaringan intra Kampus ITDA Yogyakarta.

1.5 Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian ini diantarannya sebagai berikut:

1. Mengetahui kerentanan yang dimiliki oleh Jaringan Intra Kampus ITDA.
2. Membantu memberikan evaluasi terhadap kampus sehingga dapat melakukan perbaikan terhadap celah keamanan Jaringan Intra Kampus.
3. Meningkatkan keamanan sistem informasi dan Jaringan komputer kampus.

Mencegah terjadinya serangan terhadap sistem informasi dan Jaringan komputer Kampus ITDA Yogyakrta.