BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada zaman ini perkembangan jaringan komputer sangat cepat dengan adanya berbagai kebutuhan dalam kalangan masyarakat terhadap kebutuhan jaringan. Para pengguna dapat mengakses informasi baik bersifat publik maupun pribadi. Dengan adanya internet sebagai sarana pencari informasi, maka semua jenis informasi bisa didapatkan melalui dunia maya. Perkembangan ini dapat dilihat secara nyata yang dulunya harus menunggu koran terlebih dahulu untuk mendapatkan informasi terbaru sekarang hanya dengan terkoneksi dengan jaringan internet sudah dapat memiliki informasi terbaru.

Dengan berkembangnya jaringan komputer permasalahan mengenai keamanan jaringan sangat penting dan patut untuk diperhatikan. Jaringan yang terhubung dalam sebuah perangkat jaringan masih rentan untuk diretas oleh *hacker*, baik secara DHCP atau Statis. Pada saat sebuah perangkat diberikan akses untuk menggunakan jaringan mempunyai kesempatan terhadap pengguna untuk dapat menyadap atau merusak apa saja di dalam jaringan tersebut. Dalam pembangunan sistem keamanan jaringan harus lebih diperhatikan agar dapat melindungi sumber daya yang tersimpan pada jaringan tersebut apalagi jaringan yang berada pada perusahaan atau kantor pemerintahan yang memiliki banyak data-data penting yang tersimpan di dalamnya.

Dalam penyebaran IP di suatu perusahaan biasanya digunakan *Dynamic Host Configuration Protocol* (DHCP) *server* sebagai layanan untuk pendistribusian IP secara otomatis agar mempermudah penyebaran suatu IP *address*. Untuk keamanan dalam menggunakan DHCP dapat melakukan mitigasi seperti DHCP *snooping* guna memberikan kepada *client* jaringan secara privat dengan cara IP dan MAC *Address* sudah didaftarkan pada *router*.

Router merupakan perangkat jaringan yang bertanggung jawab untuk meneruskan atau mengirimkan data dari satu *network* ke *network* yang berbeda. *Router* sering digunakan untuk menghubungkan *network* yang menggunakan

topologi *Bus*, *Ring*, dan *Star* (Sofana, 2009) dan *Switch* merupakan perangkat yang berfungsi untuk menghubungkan beberapa komputer ataupun perangkat jaringan agar dapat berbagi sumber daya. *Switch* juga merupakan perangkat keras yang memungkinkan terjadinya distribusi paket data antar komputer dalam jaringan dan mampu untuk mengenali topologi jaringan dibanyak *layer* sehingga data dapat langsung sampai ke tujuan (Sulaiman, 2016).

Penelitian sebelumnya menggunakan aplikasi *virtual* bernama *GNS3* untuk mengetahui skenario jaringan terhadap *Router Cisco*, hasil penelitian ini dapat menganalisis DHCP paket ketika mengalami DHCP *rogue* (Kurnia, 2020). Penelitian lainnya dilakukan skenario pada jaringan LAN pada *router mikrotik* yang terkena DHCP *rogue* hasil penelitian ini masih menganalisis DHCP paket kelebihannya dapat membagi DHCP secara limit (Ariyadi dan Kasim, 2018).

Penelitian sekarang menggunakan skenario serangan pada *Router Cisco* dengan teknik serangan DHCP *rogue* ketika perangkat melakukan transfer data, hasil dari transfer data akan di analisis menggunakan aplikasi berbasis *web* dengan metode statistika deskriptif dan uji anova.

Berdasarkan latar belakang tersebut, maka diangkat sebuah judul yaitu "Analisis Statistika pada Transfer Data di Jaringan *Dynamic Host Configuration Protocol* (DHCP) *Rogue* Menggunakan Deskriptif dan Uji Anova". Pada penelitian ini digunakan *router* 2800 yang berada di Laboratorium Jaringan Komputer ITDA. Dengan adanya analisis mengenai jaringan yang terkena DHCP *rogue*, maka praktisi dan administrator dapat memberikan pencegahan ketika melakukan transfer data.

1.2 Rumusan Masalah

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

1. Bagaimana pengaruh DHCP *Rogue* ketika transfer data pada perangkat *Router Cisco* 2800 dalam sebuah jaringan?

2. Bagaimana melakukan tindakan pencegahan terhadap jaringan komputer saat melakukan transfer data terhindar dari serangan DHCP *rogue*?
3. Apakah terdapat perbedaan saat transfer data pada jaringan sebelum dan setelah diserang, serta setelah dilakukan mitigasi?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah disebutkan, maka didapatkan batasan masalah sebagai berikut:

1. Perangkat yang digunakan adalah 30 buah *personal computer*, dua buah laptop, dua buah *switch*, dua buah *Router Cisco* 2800.
2. Mitigasi yang digunakan dalam penelitian ini saat terjadi penyerangan DHCP *rogue* yaitu DHCP *snooping*.
3. Parameter pengujian perbandingan dalam penelitian diukur berdasarkan nilai *metric* berupa waktu dan ukuran file.
4. Layanan data yang diuji berupa 1 *Byte*, 1 KB, 1 MB, dan 1 GB.
5. IP yang disediakan DHCP sebanyak 30 IP.
6. Transfer data dan analisis sepenuhnya menggunakan aplikasi berbasis *web*.
7. *Framework* yang digunakan yaitu *Codeigniter*, *Boostrap*, dan *JQuery*.
8. Database yang digunakan yaitu *MySql*.

1.4 Tujuan Penelitian

Penelitian ini mempunyai tujuan yaitu menguji waktu transfer dari berbagai ukuran file pada suatu jaringan yang menggunakan *Router Cisco* 2800 secara sekaligus kepada 30 *client* menggunakan jaringan lokal ketika belum terjadi penyerangan DHCP *Rogue*, saat terjadi penyerangan DHCP *Rogue*, dan setelah dimitigasi dengan menggunakan aplikasi berbasis *web*.

1.5 Manfaat Penelitian

Berdasarkan masalah dan tujuan di atas, manfaat penelitian ini adalah:

1. Penulis mendapatkan pemahaman lebih mendalam mengenai keamanan jaringan dan bagaimana cara mengatasinya.
2. Membantu praktisi jaringan untuk dapat mengetahui dan membandingkan keadaan pada saat jaringan *normal* lalu diserang kemudian dimitigasi.
3. Membantu praktisi jaringan untuk mengetahui kerugian dari penyerangan DHCP *rogue*.