

## BAB I

### PENDAHULUAN

#### 1.1 Latar Belakang

Perkembangan teknologi informasi sangat dibutuhkan oleh semua orang untuk melakukan suatu pekerjaan ataupun pembelajaran agar pekerjaan dan pembelajaran tersebut menjadi lebih mudah, apalagi teknologi informasi ini sangat penting dalam segala aspek yang terhubung dengan teknologi informasi dan komunikasi. Dengan berkembangnya teknologi secara global seperti jaringan komputer, jaringan komputer adalah kumpulan dari beberapa komputer yang saling terhubung satu sama lain, sehingga memungkinkan penggunaan dapat saling bertukar informasi berupa suara, video, dan data pada jaringan yang sama. Jaringan komputer memerlukan keamanan jaringan komputer agar terhindar dari kejahatan *cyber* yang dilakukan orang yang tidak bertanggung jawab yang mengakibatkan kehilangan data.

Beberapa instansi menggunakan jaringan komputer untuk mendukung proses pekerjaan, sehingga secara tidak langsung jaringan komputer sangat penting bagi pengguna *internet*. Dengan adanya jaringan komputer sebagai proses belajar mengajar ataupun untuk membantu pekerjaan, jaringan komputer memerlukan keamanan jaringan *internet* agar terhindar dari kejahatan *cyber* yang dilakukan oleh orang yang tidak bertanggung jawab.

Pada jurusan Teknik Komputer akan dibuat *server* jaringan baru yang berfungsi untuk mempermudah sistem pembelajaran yang menggunakan akses *internet* pada jurusan Teknik Komputer. Dengan adanya *server* baru tersebut dapat dilihat bahwa *server* tersebut belum memiliki sistem keamanan jaringan. Karena di jurusan teknik komputer belum tersedia sistem keamanan jaringan, maka penulis bermaksud ingin menggunakan *system* keamanan jaringan dengan menggunakan *DHCP Snooping*. Dengan adanya *DHCP Snooping* diharapkan dapat membantu keamanan jaringan *internet* dimana *DHCP Snooping* hanya

mengizinkan *server DHCP trusted* untuk membagikan *IP Address*, *subnetmask*, dan *gateway* pada *PC client*.

Hal tersebut dilakukan untuk menghindari adanya *cyber* yang berusaha masuk ke dalam jaringan dan penulis menggunakan alamat pada *layer 2* sebagai alamat fisik, pada jaringan komputer yang dikenal dengan nama *Media Access Control Address* atau *MAC address* bertujuan untuk mengetahui alamat *MAC address* dari masing-masing perangkat yang terhubung pada jaringan teknik komputer, karena itu *DHCP Snooping* merupakan solusi yang tepat untuk mengatasi masalah keamanan jaringan yang lebih baik.

Pada peneliti sebelumnya (Yao Tong, Shigeo Akashi: 2019) “*A Feasible Method for Realizing Leakage of DHCP Transactions under the Implementation of DHCP Snooping*”, dijelaskannya bahwa sistem keamanan jaringan menggunakan *DHCP Snooping* memiliki tugas yang cukup besar dalam meningkatkan keamanan jaringan dari kejahatan *cyber*. Tetapi, dalam penelitian tersebut penulis hanya dilakukan sebatas simulasi sehingga kita tidak dapat mengetahui bagaimana kondisi di lapangan serta penelitian tersebut hanya fokus terhadap *delay* jaringan *internet* setelah menggunakan *DHCP Snooping*.

Oleh karena itu untuk mendapatkan hasil yang lebih nyata dari penelitian sebelumnya dan untuk meningkatkan keamanan jaringan di jurusan Teknik Komputer penulis ingin menerapkan sistem keamanan *DHCP Snooping* tersebut di Teknik Komputer, dari latar belakang diatas penulis bermaksud membuat Laporan Akhir dengan Judul **“IMPLEMENTASI SISTEM KEAMANAN LOCAL AREA NETWORK MENGGUNAKAN DYNAMIC HOST CONTROL PROTOCOL (DHCP) SNOOPING PADA JURUSAN TEKNIK KOMPUTER”**.

## 1.2 Rumusan Masalah

Sesuai dengan latar belakang yang telah dijelaskan di atas, maka perumusan masalah yang akan dikaji di dalam laporan ini adalah “Bagaimana mendesain Keamanan *DHCP Snooping* Untuk Mengurangi Serangan di *Local Area Network* (LAN)?”.

## 1.3 Batasan Masalah

Agar permasalahan lebih terarah dan tidak menyimpang dari permasalahan yang diteliti, maka ditentukanlah batasan masalah sebagai berikut :

1. Keamanan jaringan dengan *DHCP Snooping* menggunakan pengalamatan IPv4.
2. Ruang lingkup pengambilan data hanya dilakukan di Teknik Komputer.
3. Desain keamanan di fokuskan pada keamanan *layer 2* pada jaringan komputer.

## 1.4 Tujuan dan Manfaat

### 1.4.1 Tujuan

Berdasarkan rumusan masalah diatas maka laporan ini bertujuan untuk mendesain keamanan jaringan pada *layer 2* dengan menggunakan *DHCP Snooping* agar jaringan komputer terhindar dari ancaman kejahatan *cyber*.

### 1.4.2 Manfaat

Adapun manfaat dari laporan ini adalah sebagai berikut :

1. *DHCP Snooping* yang terdapat pada perangkat jaringan untuk mencegah adanya *server DHCP* palsu yang mencoba memberikan alamat IP kepada *client*.
2. Melakukan pengukuran dan pengaruh penggunaan *DHCP Snooping* terhadap parameter *elapsed times*, alokasi alamat IP oleh *server* legal, *discover response time* dan *request response time*, *throughput*, serta *packet loss*.