# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Pada zaman yang modern dan serba maju ini layanan internet sudah menjadi kebutuhan yang sangat penting terhadap kehidupan manusia, dengan internet manusia dapat lebih mudah untuk melakukan pekerjaannya seperti mengelola data, mencari data, mencari informasi dan berkomunikasi. Layanan internet dapat bekerja berdasarkan infrastruktur jaringan komputer baik secara lokal ataupun global. Infrastruktur yang dibangun tentu harus didukung oleh sistem keamanan jaringan yang kuat. Sistem keamanan jaringan yang kuat sangatlah penting diterapkan pada infrastruktur jaringan, dikarenakan jika keamanan jaringan tersebut tidak mumpuni maka infrastruktur jaringan yang sudah ada dapat dengan mudah dieksploitasi oleh penyerang baik berbentuk serangan dari luar ataupun serangan dari dalam. Jika jaringan sudah berhasil dieksploitasi maka mengakibatkan kerugian seperti terganggu kinerjanya sebuah jaringan, rusaknya sumber daya jaringan yang telah ada dan kinerja jaringan yang telah dibuat menjadi tidak maksimal.

Adapun serangan pada jaringan terbagi menjadi dua jenis, yaiu serangan dari luar dan serangan dari dalam. Serangan dari dalam berbentuk penyalahgunaan akses terhadap sumber daya jaringan dan penyalahgunaan sumberdaya jaringan untuk kepentingan pribadi atau kelompok, sedangkan serangan dari luar berbentuk *flooding, hacking*, *malware, virus* dan lain-lain. Contoh serangan pada jaringan yang lebih spesifik yang dilakuman oleh *hacker* dan dapat merusak sumber daya jaringan adalah *DNS Flooding, DHCP Rogue, Bruteforce, DHCP Starvation* dan lain-lain[1].

SMK Vinama 2 Kota Bekasi adalah suatu instansi yang bergerak dibidang pendidikan. SMK Vislam Vinama 2 Kota Bekasi memiliki guru sebanyak 58 guru dan 650 siswa, SMK Islam Vinama 2 Kota Bekasi menggunakan internet sebagai sarana informasi, komunikasi baik antar guru ataupun sesama siswa. Kondisi awal jaringan SMK Vinama 2 Kota Bekasi menggunakan infrastruktur jaringan seperti

*wireline* dan *wireless.* Jaringan *wireline* yang diterapkan berfungsi untuk sarana praktikum laboratorium siswa dan jaringan *wireless* yang diterapkan berfungsi untuk kebutuhan komunikasi dan berbagi informasi staff, guru dan kepala sekolah. Dengan infrastruktur tersebut jaringan di SMK Vinama 2 Kota Bekasi sudah dapat memenuhi kebutuhan sumber daya jaringan bagi *client* nya. Pada sistem keamanan jaringan yang sudah ada pada infrastruktur jaringan tersebut untuk mengantisipasi serangan dari dalam sudah cukup baik untuk diterapkan. Contohnya seperti mengelola akses untuk menuju sumber daya jaringan, namun sistem keamanan jaringan untuk mengantisipasi serangan dari luar jaringan yang sudah ada pada infrastruktur jaringan tersebut belum maksimal keamanannya, seperti tidak ditemukannya pengamanan khusus pada *firewall* pada *device* yang difungsikan sebagai penyedia sumber daya jaringan seperti *router* dan *server*. Salah satu sumber daya jaringan yang belum diterapkannya sistem *firewall* pada *device* tersebut adalah layanan *DHCP Server*. *DHCP Server* adalah layanan jaringan yang memungkinkan *client* pada jaringan tersebut bisa mendapatkan informasi jaringan seperti *IP Address, DNS, Gateway* dan *Network Address* agar bisa berkomunikasi dengan client lainnya. Salah satu ancaman dari luar pada layanan jaringan tersebut adalah teknik serangan *DDoS* (*Denial Of Services)* yaitu serangan *DHCP Starvation.*

Kondisi jaringan *wireline* ataupun *wireless* pada infrastruktur jaringan di SMK Vinama 2 Kota Bekasi ditemukan permasalahan yaitu tidak diterapkannya metode Access Control List dengan algoritma Deep Packet Inspection pada layanan *DHCP Server* di *router* sehingga infrastruktur jaringan di SMK Vinama 2 Kota Bekasi masih rentan terhadap serangan *DDoS* yang dilakukan oleh *hacker.* Adapun salah satu serangan *DDoS* yang pernah menyerang infrastruktur jaringan di SMK Vinama 2 Kota Bekasi adalah serangan *DHCP Starvation.* Serangan *DHCP Starvation* terjadi ketika *hacker* melakukan serangan ke layanan *DHCP Server* dengan cara mengirim paket *DHCP Discover* sebanyak mungkin sehingga server merespon dengan mengirimkan paket *DHCP Offer* untuk penyerang. Setelah itu *hacker* mengirimkan paket *DHCP Request* untuk meminta *IP Address* kepada *server*. Pada langkah terakhir *server* mengirimkan paket *DHCP Ack* yaitu paket yang berisikan *IP Address* dan informasi konfigurasi lain yang dibutuhkan, sehingga serangan

tersebut dapat menghabiskan ketersediaan *IP Address* pada *IP Pool* pada sebuah router yang menyebabkan router tidak bisa memberikan *IP Address* kepada *client.* Ketika serangan tersebut terjadi, serangan tersebut menuju sebuah layanan yaitu *DHCP Server* pada sebuah *router* melalui *ethernet* satu yang bertindak sebagai *interface* ke ISP dan *ethernet* dua dan ethernet tiga yang merupakan *interface* menuju *wireline* dan *wireless* yang terhubung dengan *client*. Serangan tersebut mampu membuat *load cpu* menjadi full yang menyebabkan *router* tersebut menjadi *hang* serta menghabiskan ketersediaan *IP Address* pada *IP Leases* pada layanan *DHCP Server* tersebut. Serangan *DHCP Starvation* tersebut bisa dideteksi dan diatasi dengan menerapkan salah satu algoritma *firewall* yaitu Deep Packet Inspection. Deep Packet Inspection merupakan algoritma yang dapat memeriksa secara mendalam paket data yang masuk ataupun keluar dari sebuah jaringan dengan berdasarkan parameter yang ditetapkan. Algoritma tersebut dapat diterapkan dengan metode yang beroperasi pada *firewall* yaitu metode Access Control List.

Pada penelitian ini, peneliti menggunakan berberapa penelitian terdahulu yang menjadi referensi peneliti untuk menyelesaikan permasalahan didalam penelitian ini, adapun penelitian-penelitian tersebut adalah Penelitian oleh Haerudin dengan judul Analisa dan Implementasi Sistem Keamanan Mikrotik dari Serangan *Winbox Exploitation, Brure Force, DoS* pada tahun 2021 dengan hasil yaitu metode *penetration testing* dengan *tools kali linux* mampu menyerang *router* yang dijadikan *server* dan penerapan model keamanan dalam firewall seperti filtering yang mampu mencegah serta mengatasi serangan *DoS*. Penelitian oleh Willy Purnama Putra dan Muhammad Zulfikar Aziz dengan judul Penggunaan Metode *DHCP Snooping* Dalam Melakukan Pencegahan Terhadap *DHCP Rogue* Pada Laboratorium Informatika pada tahun 2023 dengan hasil yaitu *tools ettercap* yang dipakai untuk ujicoba serangan *DHCP Rogue* telah berhasil diujicoba dengan hasil bahwa client mendapatkan *IP Address* yang palsu dan penerapan *DHCP Snooping* mampu mengatasi serangan *DHCP Rogue* dengan syarat bahwa *switch* harus mempunyai fitur *DHCP Snooping*. Penelitian oleh Muhammad Luthfi Arsalan dengan judul Keamanan Jaringan *Wireless Fidelity (Wi-Fi)* Terhadap Serangan

*Packet Sniffing* Menggunakan *Firewall Rule* (Studi Kasus : PT Akurat Sentra Media) pada tahun 2023 dengan hasil yaitu penerapan *firewall rule* dengan metode *address list* mampu memproteksi jaringan dari serangan *ARP Spoofing*. Penelitian oleh Tamsir Ariyadi, dkk dengan judul Analisis Serangan *DHCP Starvation Attack* Pada *Router OS Mikrotik* pada tahun 2023 dengan hasil penelitian yaitu serangan *DHCP Starvation* mampu mendukung *Man In Middle Attack* sehingga *DHCP Server* akan kehabisan persediaan *IP Address* ketika *client* melakukan request *IP Address* ke server dan serangan *DHCP Starvation* tersebut akan dikombinasikan dengan *DHCP Rogue* agar client mendapat *IP Address* palsu dari *attacker*. Penelitian oleh Sarip dan Arief Setyanto dengan judul Filter Paket Berdasarkan *Differential Services Code Point* untuk pencegahan serangan *DHCP Starvation* pada tahun 2019 dengan hasil penelitian yaitu *packet filtering* dengan parameter *DSCP* yang diterapkan sudah mampu dalam mencegah serangan *DHCP Starvation* tetapi belum adanya parameter *Mac Address* dalam penelitian tersebut sehingga memungkinkan kurang efektifnya penerapan keamanan tersebut dan metode *packet filtering* tidak mampu dalam menghadapi serangan tersebut dengan skala besar sehingga memerlukan metode tambahan dalam penerapannya.

Berdasarkan penelitian-penelitian terdahulu, peneliti akan memberlakukan pembatasan koneksi paket data dan akses kontrol menggunakan algoritma Deep Packet Inspection dengan metode Access Control List. Untuk membedakan penelitian ini dengan penelitian-penelitian terdahulu maka peneliti akan menggunakan parameter *Mac Address* dan *Differentiated Service Code Point* untuk melakukan pembatasan koneksi paket data dan akses kontrol yang masuk atau keluar layanan *DHCP Server* di *Mikrotik Routerboard* dengan harapan metode access control list dan algoritma Deep Packet Inspection mampu mendeteksi dan mengatasi serangan *DHCP Starvation* yang diterapkan pada layanan *DHCP Server* di *router*. Berdasarkan latar belakang tersebut peneliti tertarik membuat penelitian yang berjudul "**DETEKSI SERANGAN *DHCP STARVATION* MENGGUNAKAN *DEEP PACKET INSPECTION* BERDASARKAN *DSCP* DAN *MAC ADDRESS* PADA JARINGAN SMK VINAMA 2 KOTA BEKASI**".

## 1.2 Identifikasi Masalah

Berdasarkan latar belakang diatas, peneliti menyimpulkan identifikasi masalah sebagai berikut:

1. Jaringan komputer baik *wireline* ataupun *wireless* di SMK Islam Vinama 2 Kota Bekasi masih rentan terhadap serangan *hacker* termasuk serangan *DDoS (Denial Of Services)* yaitu serangan *DHCP Starvation*;
2. Layanan *DHCP* Server pada Jaringan di SMK Islam Vinama 2 Kota Bekasi belum menerapkan model keamanan jaringan seperti Access Control List;
3. Belum ada penerapan algoritma Deep Packet Inspection dengan metode Access Control List pada *firewall* mengakibatkan tidak efektifnya keamanan *DHCP* Server pada Jaringan komputer di SMK Islam Vinama 2 Kota Bekasi.

## 1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah:

1. Penelitian ini membatasi paket data yang masuk ataupun keluar jaringan pada *firewall* dari *router*;
2. Pada penelitian ini tidak membahas serangan *DDoS* yang lain;
3. Penelitian ini menerapkan *Mac Address* dan *DSCP* sebagai parameter untuk cara kerja Access Control List dan Deep Packet Inspection.

## 1.4 Rumusan Masalah

Berdasarkan latar belakang diatas, penulis menyimpulkan rumusan masalah sebagai berikut, "Bagaimana membuat dan menerapkan sistem keamanan pada *firewall* pada layanan *DHCP Server* dengan menggunakan algoritma Deep Packet Inspection dan metode Access Control List dengan parameter *Mac Address* dan *Differentiated Services Code Point* yang dapat mencegah dan mengatasi serangan *DHCP Starvation*."

## 1.5 Tujuan dan Manfaat Penelitian

Tujuan dan manfaat dari penelitian yang dilakukan adalah sebagai berikut:

### 1.5.1 Tujuan Penelitian

1. Membuat sistem keamanan (*firewall*) yang bertujuan ke *DHCP Server* untuk meningkatkan keamanan di *DHCP Server*;

2. Kinerja *DHCP* Server pada *router* lebih optimal dikarenakan model keamanan dapat diterapkan dan mencegah serta mengatasi serangan *DHCP Starvation*;
3. Menerapkan model keamanan akses kontrol dan inspeksi paket data secara mendalam di *firewall* sehingga dapat meningkatkan keamanan pada *router*.

### 1.5.2 Manfaat Penelitian

1. Meningkatkan keamanan dan kenyamanan bagi *client* yang terkoneksi pada jaringan di SMK Vinama 2 Kota Bekasi dari serangan *hacker*;
2. Meningkatkan kinerja jaringan komputer, terutama layanan pada *DHCP Server* pada *router*;
3. Meningkatkan keamanan data dari pengguna jaringan yang mengakses dan terdaftar pada jaringan SMK Vinama 2 Kota Bekasi.

## 1.6 Sistematika Penulisan

Adapun sistematika penulisan tugas akhir ini terdiri dari tiga bab. Dalam penulisan tugas akhir ini dilakukan berberapa tahap yang berisi tahap-tahapan agar masalah dapat terpecahkan. Adapun rincian bab – bab nya adalah sebagai berikut,

**Bab I Pendahuluan**

Pada bab ini membahas latar belakang, identifikasi masalah, rumusan masalah, tujuan dan manfaat, batasan masalah dan sistematika penulisan.

**Bab II Landasan Teori**

Pada bab ini berisi tinjauan pustaka, mengurai materi yang mendukung judul, dan terdapat enam rangkuman penelitian terdahulu.

**Bab III Metodologi Penelitian**

Pada bab ini membahas tentang gambaran umum objek penelitian, penguraian kerangka penelitian, penguraian cara kerja algoritma deep packet inspection pada *firewall*, uraian metode pengumpulan data, uraian model penelitian dan uraian hasil analisis sistem berjalan, analisis sistem usulan serta analisis permasalahan.

**Bab IV Hasil Dan Pembahasan**

Pada bab ini membahas tentang analisis kebutuhan sistem berjalan dan usulan, implementasi sistem usulan, monitoring sistem usulan dan hasil pengujian pada sistem usulan.

**Bab V Kesimpulan Dan Saran**

Pada bab ini menguraikan tentang kesimpulan dari penelitian ini dan saran untuk pengembangan sistem pada penelitian selanjutnya.