# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Cafe Kopi Tawa merupakan salah satu tempat usaha yang bergerak dibidang penjualan coffe dan waktu operasional mulai dari jam 10 pagi sampai jam 10 malam. Cofe kopi tawa meyediakan layanaan juga dalam bentuk pelayanan jasa internet gratis bagi pengunjung via (wifi). Akses free Wifi tersebut bisa digunakan oleh pengunjung sampai 32 orang. Selain digunakan untuk pengujung, dari sisi CafeTawa proses pembayaran itu memerlukan koneksi internet yang mana dihubungkan pada jaringan sama dengan menggunkankan kabel. *CIA Triad* sendiri sebagai acuan layanan disediakan oleh CafeTawa. *CIA Triad* adalah akronim keamanan informasi yang banyak digunakan untuk pengamanan data seperti Confidentiality (Kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan). *Confidentiality* (Kerahasiaan) adalah sebuah data untuk tetap rahasia antara pengirim dan penerima, seperti contoh nya client melakukan login pada suatu website, mekanisme privasi yang paling aman adalah enkripsi. *Integrity* (Integritas) adalah data yang tidak dapat diubah atau tidak dapat diedit tanpa pengeditan tanpa diketahui. Serangan integritas adalah ketika peretas dapat mengedit data client, seperti login pada website, tanpa perubahan terdeteksi oleh website tersebut, sehingga transaksi tersebut dianggap sah. *Availability* (Ketersediaan) adalah hal penting yang perlu dilakukan untuk menjaga dan melakukan perbaikan sistem bila diperlukan serta memelihara agar sebuah sistem tetap bisa digunakan, contoh serangan *Availability* (Ketersediaan) adalah serangan *DoS* pada server. Serangan adalah ketika terlalu banyak permintaan dimuat ke server untuk membuat layanan yang dilayaninya tidak dapat diakses oleh orang lain.

Berdasarkan hasil wawancara dengan bapak Afif selaku kepala bagian divisi IT pada Cafe Kopi Tawa, Beliau menjelaskan bahwa Cafe Kopi Tawa mengalami permasalahan pada keamanan jarignan. Untuk kemanan jaringan dalam layanan internet di kafe ditemukan oleh team IT pada log akhir tahun 2020 (lampiran I) dengan menggunakan aplikasi Arp Guard, penyerangan meningkat pada bulan Desember 2020 terjadinya kejadian penyerangan dengan metode phising kurang lebih 14 kali . Untuk kasus penyerangan dari luar ada upaya untuk masuk ke dalam router Mikrotik dengan metode BruteForce. Kasus Phising terjadi pada pengujung Café dengan cara mengahlikan website yang dituju ke penyerang. Untuk kasus spoofing, penyerang menyamar sebagai router server, Ketika client mau mengakses sebuah website, data akan lewat ke penyerang, tidak langsung ke router server, dengan begitu penyerang dapat mengubah data dari client . Dalam kasus software NetCut ini sebagai penganggu ketika koneksi dipotong dengan sengaja, penggunakan software Netcut memotong koneksi pengguna dengan tujuan agar penyerang memperoleh bandwith yang

lebih besar atau hanya sekedar iseng agar pengguna yang lain tidak bisa menfaatkan fasilitas koneksi internet yang di sediakan oleh Café KopiTawa.

Kerentanan bocornya informasi karena layer aksesnya masih sebatas *Hypertext Transfer Protokol* (HTTP), lalu selain itu dengan menggunakan aplikasi *Ettercap* data dapat diliat. Kerentanan dalam protocol HTTP menjadi celah bagi peretas untuk mencuri data. Dengan menggunakan *Hypertext Transfer Protocol Secure* (HTTPS) memiliki kelebihan fungsi di bidang keamanan, HTTPS menggunakan *Secure Socket Layer* (SSL) atau *Transport Layer Security* (TLS) sebagai suyblayer dibawah HTTP layer yang biasa. Kedua protocol tersebut memberikan perlindungan yang memadai dari serangan *Man In The Middle Attcks*. Pada umumnya port yang digunakan dalam HTTPS adalah port 443.

Untuk itu maka perlu dilakukan desain sistem keamanan jaringan yang baru dengan pendekatan menggunakan cisco lifecyle (PPDIOO) dimana dalam desain keamanan yang diibangun akan diterapkan metode DNS Over HTTPS dan ARP. Metode DNS Over HTTPS merupakan sebuah protokol untuk melakukan resolusi Sistem Penamaan Domain (DNS) dengan menggunakan protokol HTTPS. Tujuan penggunaan metode ini adalah untuk melindungi privasi dan keamanan pengguna dengan mencegah serangan Man-in-the-middle. Sebuah website yang cuma penerapkan Http , Ketika client melakukan akses website www.idws.id , penyerang dapat melihat data tujuan, dan apabila sudah menerapkan Dns Over Https , website tersebut jalur data akan enkripsi .

Selain menggunakan DNS Over HTTPS atau DOH cara untu memperkuat tingkat keamanan suatu jaringan maka dapat menggunakan protocol *Address Resolution Protoco* (*Arp).* ARP merupakan sebuah protokol jaringan yang digunakan untuk mengetahui alamat perangkat keras(MAC) dari suatu suatu perangkat dari alamat IP. Ini digunakan ketika perangkat ingin berkomunikasi dengan beberapa perangkat lain di jaringan lokal (misalnya pada jaringan Ethernet yang membutuhkan alamat fisik untuk diketahui sebelum mengirim paket). Perangkat pengirim menggunakan ARP untuk menerjemahkan alamat IP ke alamat MAC. Perangkat mengirim pesan permintaan ARP yang berisi alamat IP perangkat penerima. Semua perangkat di segmen jaringan lokal melihat pesan, tetapi hanya perangkat yang memiliki alamat IP tersebut yang merespons dengan pesan balasan ARP yang berisi alamat MAC-nya. Perangkat pengiriman sekarang memiliki cukup informasi untuk mengirim paket ke perangkat penerima, Serangan bukan hanya merugikan pelanggan tetapi dapat merugikan dari pihak pengelola Café. Karena data dapat dilihat oleh penyerang.

Berdasarkan Permasalahan diatas maka dilakukan penelitian dengan judul dengan judul "**Implementasi Metode DNS Over Https Dan ARP Spoofing Untuk Keamanan Jaringan Di Cafe Kopi Tawa"** untuk meningkatkan keamanan jaringan.

## 1.2 Identifikasi Masalah

1. Terjadinya ancaman serangan Sniffing jaringan di café KopiTawa
2. Terjadinya ancaman serangan spoofing dari dalam pada jaringan Café KopiTawa
3. Belum ada sistem keamanan dari penestrasi serangan yang berasal dari luar Café KopiTawa.

## 1.3 Tujuan Penelitian

Dalam melakukan penelitian ini maksud dan tujuan penulis yang diterangkan sebagai berikut:

### 1.3.1. **Maksud**

Adapun maksud dari tujuan penelitian ini adalah implementasikan system keamanan jaringan menggunakan metode *DNS over HTTPS* (DoH) di Café KopiTawa.

### 1.3.2. **Tujuan**

Tujuan akhir yang ingin dicapai dalam penelitian ini adalah sebagai berikut.

1. Untuk meminimalkan serangan sniffing dengan menggunakan metode *DNS Over Https* (*DoH*).
2. Untuk memnimal seraganan spoffing dengan menggunakan metode *DNS Over Https* (*DoH*).
3. Untuk meningkatkan keamaanan dari serangan yang berasal dari luar dengan metode pencegahan *Ip Filtering*,

## 1.4 Batas Masalah

Batasan masalah ini untuk membatasi persoalan yang akan dihadapi agar tidak menyimpang dari apa yang diinginkan. Ada berapa batasan masalah sebagai berikut ini :

1. Ruang lingkup penelitian ini di Café KopiTawa
2. Sistem *DoH* ini hanya dapat digunakan dalam jaringan Café KopiTawa.
3. Dalam penerapan sistem keamanan jaringan ini menggunakan *Mikrotik* sebagai *server*.

## 1.5 Metodologi Penelitian

Metodologi yang digunakan pada penelitian ini yaitu dengan melalui tahap pengumpulan data sebagai berikut :

### 1.5.1. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian sebagai berikut:

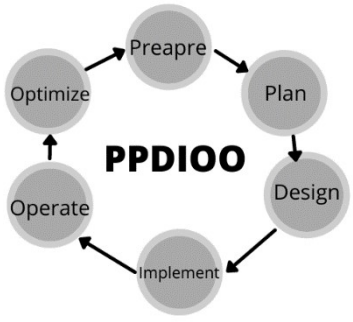
a. Literatur
   Studi literatur dilakukan dengan cara membaca dan mengkaji sumber buku, jurnal, maupun paper serta bacaan lainnya yang sesuai dan terkait dengan masalah yang sedang diteliti. Hingga saat ini, kajian tentang keamanan jaringan menggunakan metode *DNS over HTTPS (DoH)* masih jarang ditemukan dalam penjelasan berbahasa Indonesia,sehingga studi literatur yang dilakukan lebih banyak mengacu pada textbookserta website resmi yang berkaitan.

b. Observasi
   Pengumpulan data dengan peninjauan secara langsung terhadap permasalahan yang diambil

c. Wawancara
   Pengumpulan data dengan melakukan tanya jawab kepada staff Penanggung Jawab IT Café KopiTawa yang selama ini terlibat dalam pengolaan jaringan dan keamanan jaringan computer .

### 1.5.2. Metode Pengembangan Sistem

Metode yang dipakai untuk percancangan system keamanan jaringan ini adalah *Cisco Lifecycle Service* atau PPDIOO singkatan dari *Prepare*, *Plan,Design*, *Implement*, *Operate*, and *Optimize*.*Cisco Lifecycle Services* adalah cara pendekatan dengan tahap enam fase. Setiap fase mendefisikan aktifitas yang dibutuhkan untuk menerapkan penyebaran dan pengoperasian teknologi jaringan.




***Gambar 1 Prepare***

Dalam pengembangan system *PPDIOO* , fase pertama adalah *Prepare*. Pada fase ini dilakukan proses idenfikasi masalah konsep dari system yang akan diimplementasikan, jenis dan tipe penerapannya, serta komponen pendukung yang akan dikonfikurasi.

**a. Planning**

Dalam fase ini, mulai dibuat perencanaan dari hasil idenfikasi masalah, seperti komponen yang akan dibutuhkan dalam implementasi system keamanan jaringan *DNS over HTTPS (DoH)* yang mendukung dalam implementasi. Selain itu kebutuhan user akan di analisa dalam fase ini.

**b. Design**

Dalam fase ini, dirancang topoligi jaringan yang baik untuk implementasi *DNS over HTTPS (DoH)*.

**c. Implement**

Dalam fase ini, melakukan penerapan atas metode yang telah direncanakan. Dalam tahan implement, mencangkup instalasi metode yang akan digunakan sesuai dengan topologi yang sudah dirancang, konfigurasi dan pengujian pada implementasi *DNS over HTTPS (DoH)*.

**d. Operate**

Dalam fase ini, hasil dari implementasi mulai dioperasikan, untuk menyesesuaikan dengan analisa awal dengan metode implementasi dan menentukan Divisi IT yang terlibat dalam pengorperasian *DNS over HTTPS (DoH)*.

**e. Optimize**

Fase yang terakhir adalah *optimize* dimana fase ini Divisi IT berhak membuat kebijakan khusus dalam penambahan perfomasi dalam system yang telah diimplementasikan.

## 1.6 Sistemtika Penulisan

Sistemtika penulisan tugas akhir ini disusun untuk memberikan gambaran umum tentang dioptimasi system keamanan jaringan yang akan di buat.

**BAB I PENDAHULUAN**

Bab ini memaparkan tentang latar belakangan masalah , rumus masalah , batas masalah , tujuan penelitian , manfaat penelitian , dan sistemtika penulisan .

**BAB II LANDASAN TEORI**

Pada bab ini akan menjelaskan teori – teori yang berhubungan dengan *WirelessLAN ,* IEEE 802.11b/g/n , jenis topologi jaringan pada *WirelessLAN* , Media Tranmisi , Protocol *DNS* , *HTTPS* , *Arp* ,dan teori mengenai metode *Ettercap* .

**BAB III ANALISIS DAN PERANCANGAN SISTEM**

Bab ini akan menjelaskan tentang proses analisis sistem dan dioptimasi rancangan dari konfigurasi yang akan dibangun serta metode-metode yang akan diterapkan pada topic masalah yang diambil.

**BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM**

Bab ini menyajikan penerapan metode – metode yang akan digunakan dalam dioptimasi system keamanan jaringan. Serta pengujian simulasi system kemanan jaringan tersebut.

**BAB V KESIMPULAN DAN SARAN**

Bab ini berisi tentang kesimpulan dan saran yang sudah diperoleh dari hasil pengujian system serta saran untuk pengembangan system kedepannya.