

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

Dewasa ini, arah perkembangan teknologi informasi selalu menuju pada kemudahan dalam mengakses informasi. Informasi dalam bentuk tulisan, suara, gambar, dan video sangat mudah diakses dengan menggunakan internet. Pada awalnya, internet merupakan sarana untuk transfer *file*, *e-mail*, dan pemberitaan untuk suatu komunitas. Melihat kemudahan teknologi internet dalam bertukar informasi, internet makin dikenal.

Namun perkembangan internet yang sangat pesat memiliki dampak negatif salah satunya adalah keamanan informasi. Keamanan informasi inilah yang menjadi isu bagi instansi yang memiliki informasi bersifat rahasia. Seorang *hacker* bisa saja mengakses dan mengubah isi dari informasi tersebut. Berdasarkan laporan yang diterima oleh Hackmageddon, jumlah *cyber crime* setiap tahun mengalami kenaikan, yaitu pada tahun 2016 terjadi *cyber crime* sebanyak 72,1% dan pada tahun 2017 naik menjadi 77,4%, sedangkan data pada tahun 2018 tercatat bulan Oktober 2018 kejahatan *cyber crime* naik menjadi 77,9 [1].

*Cyber crime* merupakan kejahatan yang dilakukan pada dunia maya dengan menggunakan teknologi komputer atau jaringan komputer. Kejahatan yang berupa *cyber crime* antara lain penipuan, pencurian identitas, pencurian data, menembus komputer server tanpa otoritas, menyerang komputer dengan *virus* atau *malware*. Dalam *cyber crime* terdapat beberapa tipe serangan yang sering digunakan oleh

*hacker*. *Targeted attack* dan *malware* merupakan tipe serangan yang cukup sering digunakan. *Targeted attack* adalah serangan setelah mempelajari kelemahan sistem dari target, Kelemahan sistem yang dapat dieksploitasi oleh *hacker* adalah *outdated software*, struktur jaringan, serta lokasi server dan *backup server*, berdasarkan laporan yang diterima oleh Hackmageddon persentase *cyber crime* dengan metode *targeted attack* pada bulan oktober 2018 mencapai 16,8%. *Malware* adalah suatu program untuk merusak dengan menyusup ke sistem komputer, berdasarkan laporan yang diterima oleh Hackmageddon persentase *cyber crime* dengan metode *malware* pada bulan oktober 2018 mencapai 28.3%. [1][2][3].

STIE Putra Bangsa merupakan sekolah tinggi ilmu ekonomi di Kabupaten Kebumen yang sudah memiliki akreditasi B. STIE Putra Bangsa terdapat direktorat yang bertugas mengelola dan mengolah data akademik civitas akademika di STIE Putra Bangsa, juga beberapa direktorat lainnya yang saling berkesinambungan. Oleh karena itu, jaringan di STIE Putra Bangsa dituntut untuk memiliki tingkat keamanan dan ketersediaan jaringan yang baik. Hingga saat ini, jaringan di STIE Putra Bangsa masih menggunakan struktur *flat network*. Akibatnya tidak ada segmentasi antara jaringan pimpinan, direktorat, mahasiswa, dan pengunjung/tamu sehingga rentan terhadap serangan dan penyadapan. Maka dari itu, diperlukan adanya pembagian hierarki pada jaringan STIE Putra Bangsa untuk membatasi akses *host*. Struktur *flat network* juga tidak menyediakan jalur *backup* sehingga apabila *router* utama mati maka seluruh jaringan akan berhenti bekerja.

Salah satu usaha untuk meningkatkan keamanan dan ketersediaan jaringan di STIE Putra Bangsa yaitu dengan menerapkan *hierarchical network*. *Hierarchical*

*network* merupakan struktur jaringan internal yang terbagi beberapa jaringan kecil dengan menggunakan beberapa *core switch*. Kelebihan dari *hierarchical network* adalah administrator jaringan dapat mengatur laju dan arah informasi serta membatasi akses antar jaringan, serta apabila salah satu *core switch* mati atau jalur kabel terputus maka jaringan akan tetap bekerja secara normal. STIE Putra Bangsa jika menerapkan struktur jaringan *hierarchical network* dapat membagi *network address* yang tersedia dan membuat *access control list (ACL)* untuk membatasi akses tiap perangkat pada jaringan internal, sehingga mengurangi masalah keamanan dan kelemahan sistem yang dapat dieksploitasi oleh *hacker*.

*Hierarchical network* pada STIE Putra Bangsa menjadikan adanya ketersediaan jaringan yang mumpuni dengan menggunakan *Two-Tier Collapsed Core Design* dan segmentasi antar *host* sehingga mengurangi resiko keamanan, seperti pencurian data, penyadapan, penyebaran *malware*, dan *targeted attack*. Hasil dari penelitian ini adalah rancangan *hierarchical network* STIE Putra Bangsa pada Cisco Packet Tracer 7.2. *Hierarchical network* tersebut menerapkan konsep VLAN dan kebijakan ACL sebagai kebijakan akses *host* dalam jaringan serta penyaringan paket dari luar jaringan.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, didapatkan beberapa rumusan masalah sebagai berikut.

1. Bagaimana meningkatkan keamanan jaringan Sekolah Tinggi Ilmu Ekonomi (STIE) Putra Bangsa ?.



2. Bagaimana meningkatkan ketersediaan jaringan Sekolah Tinggi Ilmu Ekonomi (STIE) Putra Bangsa ?.

### 1.3 Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Hasil dari penelitian ini adalah usulan rancangan jaringan komputer pada Microsoft Visio Professional 2016 dan simulasi jaringan *hierarchical network* STIE Putra Bangsa pada Cisco Packet Tracer 7.2.
2. Implementasi jaringan dan simulasi jaringan menggunakan Cisco Packet Tracer 7.2.
3. Ruang lingkup desain jaringan yang digunakan adalah jaringan lokal pada Gedung STIE Putra Bangsa.
4. Sistem Operasi yang digunakan untuk menjalankan Cisco Packet Tracer 7.2 adalah Windows 10 64bit.
5. Perangkat jaringan yang digunakan dalam desain jaringan *hierarchical network* pada STIE Putra Bangsa yaitu menggunakan perangkat CISCO.
6. Metode pengembangan jaringan yang digunakan menggunakan metode NDLC sampai tahap *simulation prototyping*.
7. Penelitian ini tidak dapat memberikan bukti terhadap serangan *hacker* karena penelitian ini hanya sampai tahap simulasi jaringan.

### 1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Mengkaji desain jaringan *hierarchical network* pada STIE Putra Bangsa
2. Mengkaji kebutuhan VLAN pada STIE Putra Bangsa
3. Mengkaji *access control list* untuk membatasi hak akses tiap anggota VLAN dengan Cisco Packet Tracer 7.2.
4. Mengkaji HSRP untuk meningkatkan ketersediaan jaringan pada STIE Putra Bangsa
5. Mengkonfigurasi dan membuat simulasi desain jaringan dengan Cisco Packet Tracer 7.2.
6. Mengevaluasi hasil simulasi yang telah dilakukan.

### **1.5 Manfaat Penelitian**

Manfaat penelitian yang dapat diambil dari penelitian ini adalah :

1. Pihak STIE Putra Bangsa dapat menerapkan rancangan jaringan yang dibuat pada penelitian ini.
2. Kampus lain atau instansi lain dapat menerapkan rancangan *hierarchical network* dari hasil penelitian ini.
3. Menambah kepercayaan civitas akademika STIE Putra Bangsa terhadap keamanan informasi pada STIE Putra Bangsa.

### **1.6 Metode Penelitian**

Metode yang digunakan oleh penulis dalam memperoleh data-data untuk penelitian adalah sebagai berikut :

## **1.6.1 Metode Pengumpulan Data**

### **1.6.1.1 Metode Pustaka**

Pengumpulan data dari sumber ilmiah baik itu buku, jurnal, artikel, dan karya ilmiah lainnya yang berkaitan dengan tema penelitian baik di perpustakaan atau di internet.

### **1.6.1.2 Wawancara**

Melakukan wawancara kepada pegawai khususnya Staff IT Sekolah Tinggi Ilmu Ekonomi (STIE) Putra Bangsa untuk mendapatkan informasi yang dibutuhkan dalam penelitian.

## **1.6.2 Analisis dan Perancangan**

### **1.6.2.1 Analisis Kondisi Awal**

Analisis Kondisi Awal digunakan untuk mengumpulkan informasi tentang kondisi awal jaringan, kebutuhan perangkat yang terhubung ke jaringan, dan denah ruangan gedung Sekolah Tinggi Ilmu Ekonomi (STIE) Putra Bangsa. Informasi tersebut kemudian digunakan dalam proses perancangan jaringan agar sesuai dengan kebutuhan jaringan dan rencana mendatang Sekolah Tinggi Ilmu Ekonomi (STIE) Putra Bangsa.

### 1.6.2.2 Perancangan

Melakukan perancangan untuk sistem jaringan baru yang akan digunakan pada penelitian.

## 1.7 Metodologi Penelitian

Metodologi penelitian yang digunakan adalah metode pengembangan jaringan dengan model *Network Development Life Cycle* (NDLC). Berikut adalah tahapan dari NDLC.

### a. *Analysis*

Tahap analisis dilakukan dengan menganalisa kebutuhan, analisa permasalahan yang muncul, dan analisa kondisi jaringan awal. Metode yang digunakan pada tahap ini adalah metode pengumpulan data dengan wawancara dan survey langsung ke lokasi.

### b. *Design*

Berdasarkan data – data yang didapatkan sebelumnya, tahap *design* ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi, desain akses data, desain layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun.



**c. Simulation Prototype**

Merupakan tahapan berupa pembuatan simulasi dengan aplikasi simulasi jaringan seperti GNS3 dan Cisco Packet Tracer. Pembuatan simulasi dimaksudkan untuk melihat kinerja awal dari jaringan yang akan dibangun dan sebagai bahan presentasi..

**d. Implementation**

Merupakan tahap penerapan semua hal yang telah direncanakan sesuai desain dan analisis yang telah dilakukan sebelumnya. Tahap ini diawali dengan testing untuk memastikan bahwa sistem siap untuk digunakan, implementasi sekaligus menilai berhasil atau gagalnya sistem untuk digunakan setelah berhasil di uji coba sebelumnya.

**e. Monitoring**

Tahapan monitoring merupakan tahapan yang menjamin agar jaringan komputer dapat berjalan sesuai dengan keinginan dan tujuan dari tahap awal analisis. Monitoring dapat berupa kegiatan pengamatan pada :

- a. Infrastruktur *hardware* : dengan mengamati kondisi *reliability* (kehandalan) sistem yang telah dibangun ( $reliability = performance + availability + security$ ).
- b. Memperhatikan jalannya paket data di jaringan (pewaktuan, *latency*, *peektime* dan *throughput*).
- c. Metode yang digunakan untuk mengamati "kesehatan" jaringan dan komunikasi secara umum secara terpusat atau tersebar.



#### *f. Management*

Tahapan manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (*policy*). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga. *Policy* akan sangat tergantung dengan kebijakan level *management* dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau *alignment* dengan strategi bisnis perusahaan.

### **1.8 Sistematika Penulisan**

Sistematika penulisan dalam penyelesaian skripsi terdiri dari lima bab. Berikut sistematika penulisan yang dideskripsikan dalam bentuk bab :

#### **BAB I PENDAHULUAN**

Bab ini berisi tentang latar belakang mengapa penelitian ini dilakukan. Selain itu, dalam bab ini dibahas tentang latar belakang, rumusan masalah, batasan masalah, Tujuan penelitian, Manfaat penelitian, Metode penelitian, dan Sistematika penelitian.

#### **BAB II DASAR TEORI**

Bab ini berisi tentang penelitian sebelumnya yang berkaitan dengan penelitian ini serta teori-teori yang relevan dengan penelitian ini.

#### **BAB III METODOLOGI PENELITIAN**

Bab ini berisi tentang metode yang digunakan dalam penelitian ini, seperti sumber data, alat penelitian, dan alur penelitian.

**BAB IV IMPLEMENTASI DAN PEMBAHASAN**

Bab ini berisi implementasi yang didapatkan dari penelitian yang telah dilakukan beserta pembahasannya.

**BAB V PENUTUP**

Bab ini berisi kesimpulan akhir dari penelitian yang dilakukan dan saran-saran untuk pengembangan penelitian selanjutnya.

