BAB I
PENDAHULUAN

1.1. Latar Belakang Penelitian

Jaringan komputer menjadi kebutuhan utama dalam pemanfaatan sistem informasi. Dengan adanya jaringan komputer, maka setiap data dan informasi dapat dialirkan sesuai kebutuhan. Pengguna jaringan komputer menggunakan *hardware* atau *software* untuk dapat saling berbagi data dan informasi yang diperlukan. Namun seiring berkembangnya zaman, kecanggihan Ilmu Pengetahuan dan Teknologi (IPTEK) telah memasuki berbagai sektor di kehidupan masyarakat. Mulai dari sektor kecil seperti usaha *profit* atau *non-profit*, kemudian sektor besar seperti perbankan, kesehatan, pemerintahan dan salah satunya pendidikan dalam lingkup kampus atau jenjang perkuliahan. Semakin banyaknya orang yang mengakses teknologi untuk memperoleh informasi, maka memungkinkan adanya ketidakamanan suatu sistem jaringan pada perangkat yang digunakan. Sejalan dengan pendapat Silitonga, dkk (2014) yang menyatakan bahwa salah satu masalah yang sering terjadi dengan jaringan komputer adalah banyaknya pengguna yang menggunakan jalur jaringan. Akibatnya, jaringan akan mengalami kemacetan jika tidak ada pengaturan, yang mengakibatkan semua pengguna jaringan tidak dapat mengaksesnya. Dengan demikian, untuk mencegah pihak-pihak yang mencoba memanfaatkan kelemahan sistem jaringan tersebut serta memberikan kesadaran kepada pengguna tentang pentingnya sistem informasi, maka diperlukan keamanan siber yang kuat.

Keamanan siber didefinisikan sebagai upaya untuk melindungi informasi, sistem, dan perangkat keras yang digunakan, disimpan, dan dipertukarkan untuk memastikan integritas, kerahasiaan, dan ketersediaan data (Alkhudhayr, dkk, 2019). Keamanan siber penting untuk diperhatikan agar dapat menghindari terjadinya kejahatan siber. Adapun jenis-jenis kejahatan siber telah dijelaskan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) yaitu terdapat tujuh jenis kejahatan yang diklasifikasikan sebagai kejahatan siber diantaranya meretas (*hacking*), penyadapan ilegal, pencemaran nama baik (*defacing*), pemerasan atau ancaman, pencurian dokumen elektronik, pencurian informasi elektronik, dan pencurian identitas. Data e-MP

Robinopsnal Bareskrim Polri menyebutkan bahwa sejak 1 Januari hingga 22 Desember 2022, polisi menindak 8.831 kasus kejahatan siber (Pusiknas Bareskrim Polri, 2021). Selanjutnya Ketua Komite I DPD RI Akhmad Muqowam mengungkapkan bahwa tingkat kejahatan siber di Indonesia masuk peringkat ke-2 di dunia (Kominfo, 2024). Pelaku kejahatan siber telah memanfaatkan kesempatan untuk menyerang individu atau organisasi dengan berbagai cara, sehingga untuk mengatasinya diperlukan keamanan siber yang efektif. Hal ini meliputi adanya analisis terperinci, implementasi, pembaharuan dan pemantauan (Herdiana, 2021). Dapat disimpulkan bahwa untuk menjaga keamanan siber, setiap pengguna sistem informasi perlu mengadopsi praktik keamanan yang baik dan efektif serta menggunakan analisis keamanan yang dapat meningkatkan kesadaran terhadap kemungkinan risiko siber.

Menteri Ketenagakerjaan Republik Indonesia telah mengatur tentang standar Kompetensi Kerja Nasional Indonesia (KKNI) kategori informasi pada bidang keamanan informasi sebagai upaya penyesuaian dengan percepatan transformasi masyarakat terhadap budaya digital. Hal tersebut dilakukan sebagai acuan bagi setiap individu yang melakukan fungsi-fungsi keamanan informasi agar memiliki kompetensi yang baik dalam menghadapi kejahatan siber. Berdasarkan Keputusan Menteri Nakertrans RI No. 3, tahun 2016, mengenai cara penetapan SKKNI, Standar Kompetensi Kerja Nasional Indonesia (SKKNI) adalah rumusan kemampuan kerja yang mencakup aspek pengetahuan, keterampilan dan atau keahlian, serta sikap kerja yang relevan dengan pelaksanaan tugas dan persyaratan pekerjaan yang ditetapkan, sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Adapun tenaga ahli yang menangani desain, pelaksanaan, pengawasan, dan pengembangan setiap langkah keamanan yang diperlukan untuk melindungi jaringan komputer perusahaan dikenal sebagai *Network Security Analyst* (NSA) (Exaplan Training, 2022). Dalam dunia pendidikan khususnya jenjang perkuliahan bidang sistem dan teknologi informasi, pada SKKNI disebutkan bahwa adanya indikator kompetensi yang perlu dimiliki oleh seorang calon *Network Security Analyst* (NSA) yaitu salah satunya dengan mempelajari tentang keamanan jaringan.

Koordinator TIM KKNI Direktorat Pembelajaran dan Kemahasiswaan Direktorat Jenderal Pendidikan Tinggi menyatakan bahwa lulusan S1, dalam Kerangka Kualifikasi Nasional Indonesia (KKNI), ditempatkan pada jenjang 6. Posisi ini menandakan bahwa kualifikasi lulusan Strata-1 (S1) harus mencerminkan kemampuan untuk menguasai konsep teoritis bidang pengetahuan dan keterampilan tertentu secara umum dan konsep teoritis bagian khusus dalam bidang pengetahuan dan keterampilan secara mendalam. Lulusan S1 pada jenjang 6 KKNI memiliki kompetensi mengaplikasikan, mengkaji, membuat desain, memanfaatkan IPTEKS dan menyelesaikan masalah. Pemerintah Indonesia sudah berusaha untuk meningkatkan kesadaran tentang penegakan keamanan siber, namun pendidikan tentang keamanan siber ini secara khusus belum diberikan secara memadai (Mahendra, 2023). Hal tersebut sesuai dengan hasil observasi yang telah dilakukan oleh peneliti.

Fakta di lapangan menunjukkan bahwa ditemukannya layanan kualitas pembelajaran praktik yang belum melibatkan penggunaan *jobsheet* berisikan materi konfigurasi MikroTik tentang keamanan siber sesuai dengan KKNI jenjang 6 dan SKKNI *Network Security Analyst*. Hal ini meyakinkan bahwa memang diperlukannya pengadaan muatan materi tentang keamanan siber ke dalam kurikulum pendidikan agar siswa di berbagai wilayah dapat memahami tantangan keamanan siber di era digital. Khususnya bagi mahasiswa pada bidang sistem teknologi dan informasi sebagai calon *Network Security Analyst* (NSA).

Berdasarkan uraian permasalahan yang telah dipaparkan, peneliti melakukan penelitian kolaborasi dengan peneliti lain untuk merancang sebuah *website* media pembelajaran berisi kompetensi jaringan komputer dengan menggunakan pendekatan KKNI yang telah diintegrasikan dengan SKKNI. Dalam penelitian kolaborasi ini, peneliti berfokus pada perancangan dan analisis *Quality of Service* konfigurasi MikroTik tentang keamanan siber yang disesuaikan dengan SKKNI *Network Security Analyst*. Peneliti menduga bahwa konfigurasi MikroTik yang telah dirancang perlu dianalisis *Quality of Service* untuk memastikan kestabilan dan kinerja yang optimal agar dapat menjadi materi yang layak dalam pembuatan *jobsheet* sebagai media pembelajaran praktik. Maka dapat disimpulkan bahwa penelitian mengenai konfigurasi keamanan siber penting untuk dilakukan.

Sehingga peneliti menetapkan judul penelitian ini yaitu "Analisis Quality of Service (QoS) Pada Konfigurasi Keamanan Siber Sebagai Muatan Media JobSheetKu."

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan, rumusan masalah yang menjadi fokus dan akan diselesaikan, yaitu:

1.2.1. Bagaimana desain konfigurasi MikroTik yang memuat keamanan siber sesuai SKKNI *Network Security Analyst*?

1.2.2. Bagaimana hasil pengujian *Quality of Service* (QoS) pada jaringan setelah konfigurasi diterapkan?

1.3. Batasan Masalah

Berdasarkan identifikasi dan rumusan masalah, diperlukan Batasan masalah supaya alur penelitian dapat dilakukan sesuai prosedur penelitian yang telah direncanakan. Berikut merupakan Batasan masalah untuk penelitian ini:

1.3.1. Dalam Standar Kompetensi Kerja Nasional Indonesia (SKKNI) terdapat banyak judul unit tentang jaringan, dalam penelitian ini peneliti menggunakan SKKNI *Network Security Analyst.*

1.3.2. Dalam merancang konfigurasi keamanan jaringan terdapat banyak konfigurasi yang digunakan, dalam penelitian ini peneliti menggunakan konfigurasi pencegahan *Brute Force* dan *Port Scanning* sebagai konfigurasi yang digunakan.

1.4. Tujuan Penelitian

Berikut merupakan tujuan dari penelitian ini:

1.4.1. Merancang konfigurasi MikroTik yang memuat keamanan siber yang sesuai dengan SKKNI *Network Security Analyst* yang dapat menjadi materi pembuatan *jobsheet* dalam pembelajaran Mata Kuliah Jaringan dan Komputer Program Studi Pendidikan Sistem dan Teknologi Informasi Universitas Pendidikan Indonesia Kampus Purwakarta untuk memberikan pembelajaran mengenai keamanan siber juga tetap meningkatkan kesadaran siswa terhadap keamanan siber.

1.4.2. Melakukan pengujian *Quality of Service* (QoS) untuk mengukur dan mengevaluasi kinerja konfigurasi MikroTik yang telah dibuat juga memastikan konsistensi konfigurasi dalam berbagai kondisi jaringan.

1.5. Manfaat Penelitian

Penelitian ini memiliki dampak positif secara teoritis dan praktis bagi para mahasiswa. Selain itu, penelitian ini menghasilkan suatu produk, yaitu konfigurasi MikroTik yang berbasis SKKNI. Konfigurasi MikroTik dirancang menjadi materi isi pembuatan JobSheet untuk meningkatkan kompetensi kerja mahasiswa Universitas Pendidikan Indonesia Kampus Purwakarta yang nantinya dapat digunakan di dunia kerja.

1.5.1. Manfaat Teoretis

Menerapkan materi keamanan siber yang dapat membantu mahasiswa mempelajari keamanan siber juga meningkatkan kesadaran mengenai keamanan siber

1.5.2. Manfaat Praktis

1) Tenaga Pendidik, mampu menjadikan konfigurasi MikroTik yang dibuat sebagai acuan dan referensi dalam pembuatan konfigurasi lainnya.
2) Peneliti, pengalaman merupakan suatu proses yang melibatkan pembelajaran dan pengembangan teknologi. Tujuan utamanya adalah untuk mengaplikasikan hasil-hasil pembelajaran dan pengembangan tersebut kepada peserta didik. Hal ini bertujuan meningkatkan kecakapan mereka sebagai bekal yang relevan dan komprehensif dalam menghadapi tuntutan dunia kerja.
3) Peneliti Selanjutnya. penelitian ini diharapkan dapat dijadikan sebagai rujukan faktual dalam perancangan konfigurasi MikroTik

1.6. Struktur Organisasi Skripsi

Struktur organisasi skripsi merupakan sistematika penulisan penelitian yang memberikan gambaran kandungan pada setiap babnya. Struktur organisasi skripsi pada penelitian ini berisi BAB I hingga BAB V sebagai berikut:

1) Bab I: Pendahuluan

   Bab ini berisi tentang latar belakang, identifikasi, rumusan, dan batasan masalah, tujuan penelitian, serta manfaat penelitian.

2) Bab II: Kajian Pustaka

Bab ini berisi tentang kajian teoritis, penelitian terdahulu dan metode penelitian yang mendukung penelitian ini.

3) Bab III: Metode Penelitian

   Bab ini berisi tentang jenis penelitian, pengumpulan data, prosedur penelitian, serta analisis data.

4) Bab IV: Temuan dan Pembahasan

   Bab ini berisi tentang hasil dan pembahasan mengenai penelitian yang dilakukan

5) Bab V: Simpulan, Implikasi, serta Rekomendasi

   Bab ini berisi simpulan, implikasi, dan rekomendasi yang didasarkan pada hasil penelitian yang diperoleh.