BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi jaringan komputer di Indonesia sudah sangat berkembang, dikutip dari laporan Kominfo pada tahun 2021, pengguna internet di Indonesia sudah mencapai 202,6 juta pengguna, naik sebanyak 11 persen dari tahun sebelumnya (Ditjen Aptika, 2021). Hal ini membuat keamanan informasi data pribadi perlu ditingkatkan agar terhindar dari kejahatan siber yang makin marak terjadi. Seperti yang terjadi pada kasus kebocoran data kependudukan Indonesia sebanyak 279 juta dan di jual pada forum peretas, kebocoran aplikasi E-HAC, sampai kebocoran NIK dan sertifikat vaksin Presiden Joko Widodo (*Rentetan Kasus Dugaan Kebocoran Data Kesehatan Pemerintah*, 2021).

Menurut laporan pada tahun 2021, sebanyak 1.637.973.022 serangan atau anomali yang terjadi di jaringan internet di Indonesia (Badan Siber dan Sandi Negara, 2022). Pada laporan tersebut terdapat beberapa tipe serangan dengan 3 serangan teratas yaitu Mylobot Botnet, Protocol-Scada Moxa, dan MiningPool. Pada serangan Mylobot memungkinkan penyerang untuk mengambil kendali penuh atas sistem pengguna dan melakukan serangan terhadap jaringan komputer, seperti DNS Spoofing, DHCP Starvation, dan serangan lainnya yang dapat melumpuhkan jaringan komputer. *Protocol-Scada Moxa* yang dapat melakukan injeksi malware dan melakukan serangan Denial-of-Service (DOS) dan Man-in-the-Middle attack pada sistem yang dapat mempengaruhi operasi dan stabilitas pada sistem. Sedangkan MiningPool adalah suatu program jahat yang digunakan untuk melakukan penambangan mata uang crypto dengan memanfaatkan sumber daya yang dimiliki korban, hal ini mengakibatkan perangkat mengalami penurunan daya, memori dan kegunaan operasional pada perangkat korban (Badan Siber dan Sandi Negara, 2022). Hal ini dapat menjadi masalah besar jika tidak ditangani dengan serius terlebih dalam lingkup organisasi yang menggunakan jaringan komputer sebagai sarana operasional.

Mengingat serangan siber yang terjadi di Indonesia sangat banyak, maka perlu adanya sistem untuk mendeteksi dan mencegah serangan siber yang terjadi. Salah satu solusi sistem keamanan pada jaringan komputer adalah IDS *Intrusion Detection System* dan IPS *Intrusion Prevention System* yang dapat mencegah serangan siber. IDS adalah sebuah perangkat lunak atau perangkat keras atau kombinasi antara keduanya yang dapat mendeteksi gangguan dalam suatu sistem atau jaringan. Sedangkan IPS adalah sistem keamanan jaringan atau sistem pencegah ancaman yang memindai lalu lintas jaringan dan mencegah eksploitasi akses yang tidak sah dari suatu aplikasi atau sistem (Gaddam and Nandhini, 2017).

Selain penerapan IDPS, setiap organisasi perlu untuk melakukan asesmen penilaian terhadap kesiapan keamanan internalnya. Tujuan untuk melakukan asesmen ini adalah sebagai parameter sejauh mana organisasi telah melakukan penerapan sistem informasi dan kemanan jaringan komputer. Salah satu cara untuk melakukan asesmen tersebut dengan memanfaatkan Indeks KAMI (Keamanan Informasi) yang dibuat oleh BSSN. Indeks KAMI merupakan alat bantu untuk melakukan evaluasi terhadap parameter keamanan jaringan komputer dan tingkat penerapan pada SNI ISO/IEC 27001:2009 (Yunella *et al.*, 2019). Pengisian survei Indeks KAMI dilakukan oleh tim IT internal perusahaan untuk mendapatkan data dan penilaian yang sesuai. Setelah pengisian survei dilakukan maka akan menghasilkan penilaian yang menunjukan tingkat kesiapan organisasi tersebut dari sisi keamanan jaringan.

Salah satu organisasi dibidang pendidikan yang memanfaatkan jaringan komputer sebagai salah satu sarana operasional utama adalah Politeknik XYZ Jaringan komputer di Politeknik ini digunakan tidak hanya untuk sarana operasional internal namun juga digunakan secara luas oleh para sivitasnya. Jaringan komputer pada Politeknik XYZ ini digunakan oleh kurang lebih 500+ pengguna yang terdiri dari sivitas dan staff Politeknik XYZ. Selain itu Politeknik XYZ juga memiliki 3 server internal yang digunakan untuk operasional. Semua kegiatan belajar mengajar dan administrasi sangat bergantung pada jaringan komputer.

Untuk melindungi sivitas dan memperkuat sistem keamanan pada jaringan komputer yang ada di Politeknik XYZ, maka perlu adanya penerapan sistem pendeteksi dan pencegahan terhadap serangan pada jaringan komputer Politeknik XYZ, serta melakukan penilaian terhadap kesiapan Politeknik XYZ dalam penerapan sistem keamanan yang telah dilakukan. Dengan melakukan Penerapan IDPS sebagai sistem pendeteksi dan pencegahan dalam jaringan komputer, serta melakukan penilaian kesiapan terhadap sistem keamanan dengan menggunakan Indeks KAMI sebelum dan sesudah penerapan IDPS pada jaringan komputer.

Berdasarkan latar belakang tersebut, penulis melakukan penelitian dengan judul **IMPLEMENTASI INTRUSION DETECTION AND PREVENTION SYSTEM DAN IMPLIKASINYA PADA INDEKS KEAMANAN INFORMASI STUDI KASUS: POLITEKNIK XYZ**, dengan tujuan untuk membangun IDPS pada lingkup Politeknik, serta melakukan analisa dan evaluasi terhadap penilaian Indeks KAMI.

1.2 Identifikasi Masalah

Berdasarkan analisa yang telah penulis lakukan, terdapat beberapa masalah yang menjadi pokok penulisan dalam laporan ini terdiri dari:

1. Bagaimana membangun sistem keamanan untuk mendeteksi dan mencegah serangan siber pada Politeknik XYZ?
2. Bagaimana melakukan analisa dan evaluasi tingkat kesiapan pengamanan informasi dengan indeks KAMI pada Politeknik XYZ?

1.3 Tujuan Penelitian

Adapun Tujuan Penelitian yang akan dicapai penulis adalah sebagai berikut:

1. Membangun sistem keamanan dengan IDPS untuk mendeteksi dan mencegah serangan siber di dalam jaringan Politeknik XYZ
2. Melakukan analisis tingkat kesiapan sistem keamanan informasi dengan indeks KAMI

1.4 Manfaat Penelitian

1. Meningkatkan keamanan di dalam jaringan internal Politeknik XYZ terhadap serangan siber
2. Memberikan keamanan tambahan terhadap jaringan komputer dalam jaringan internal Politeknik XYZ
3. Mengetahui tingkat kesiapan sistem keamanan berdasarkan penilaian Indeks KAMI

1.5 Lingkup Tugas Akhir

Lingkup tugas akhir dalam penelitian ini adalah sebagai berikut:

1. Implementasi dilakukan di dalam jaringan internal Politeknik XYZ
2. Analisa dan evaluasi Indeks KAMI di lakukan dalam jaringan internal Politeknik XYZ

1.6 Sistematika Penulisan Tugas Akhir

Sistematika penulisan yang digunakan dalam penelitian ini terbagi menjadi 5 bab yaitu:

BAB 1 PENDAHULUAN

Pada bab ini menjelaskan Latar Belakang, Identifikasi Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Kerangka Berpikir, dan Sistematika Penulisan Tugas Akhir.

BAB 2 LANDASAN TEORI

Pada bab ini berisi teori-teori yang akan digunakan dalam penelitian ini sebagai pendukung penulisan penelitian ini.

BAB 3 METODE PENELITIAN

Pada bab ini menjelaskan rencana penelitian, objek penelitian dan metode yang digunakan dalam penelitian dalam pengumpulan data pada penelitian ini.

BAB 4 HASIL DAN PEMBAHASAN

Pada bab ini memuat pembahasan mengenai sistem yang dibuat dan hasil implementasi

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini menguraikan kesimpulan dan saran yang terkait dengan penelitian yang telah dilakukan.