BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan jaringan komputer telah berkembang pesat dalam beberapa dekade terakhir. Pada mulanya, penggunaannya terbatas pada lingkungan militer dan instansi pemerintah. Namun, dengan kemajuan teknologi, jaringan komputer mulai dikenal luas dan dimanfaatkan di berbagai sektor (Nono Heryana et al., 2023). internet dan jaringan komputer di era saat ini menawarkan kemudahan dan manfaat bagi para pengguna dalam membagikan sumber daya serta informasi melalui komputer-komputer yang terhubung, baik dalam jaringan berskala lokal maupun global (Amir et al., 2023). Seiring dengan semakin meluasnya penggunaan internet, berbagai permasalahan terkait keamanan jaringan mulai bermunculan dan menjadi ancaman yang semakin serius. Kondisi ini menimbulkan kekhawatiran, baik bagi pengguna internet secara umum maupun bagi perusahaan dan lembaga yang bergerak di bidang teknologi informasi, karena data penting dapat sewaktu-waktu diretas oleh pihak yang tidak bertanggung jawab. Oleh karena itu, agar akses internet di perusahaan atau lembaga tetap berjalan lancar, diperlukan perhatian khusus terhadap sistem jaringan dan keamanannya (Supriadi et al., 2024).

Seiring dengan pesatnya perkembangan teknologi, para pengguna pun dituntut untuk terus mengikuti kemajuan tersebut. Sejalan dengan perkembangan itu, aspek keamanan dari teknologi juga menjadi perhatian penting. Keamanan sendiri merupakan upaya yang dilakukan untuk menjaga dan melindungi informasi

di dalamnya, dengan tetap mengutamakan kerahasiaan (Armadhani et al., 2022). Berdasarkan definisi dari Organisasi *Internasional* untuk Standardisasi, keamanan jaringan komputer merujuk pada upaya perlindungan terhadap perangkat keras, perangkat lunak, serta sumber daya data yang terdapat dalam sistem komputer (Informatika et al., 2025). Keamanan jaringan komputer bukan hanya merupakan bagian penting dari sistem informasi, tetapi juga berperan dalam menjaga kerahasiaan, integritas data, serta memastikan layanan tetap tersedia bagi para pengguna (Pradita & Pramono, 2024). Ketidakamanan sistem dapat menimbulkan dampak merugikan baik bagi penyedia maupun pengguna (Furqan et al., 2023). Sangat penting bagi sebuah jaringan komputer untuk menjaga keamanannya dengan baik. Apabila keamanan tersebut diabaikan, celah atau kelemahan dalam jaringan bisa dimanfaatkan oleh pihak tak dikenal untuk mengakses sistem tanpa izin, yang berisiko menimbulkan berbagai kerugian seperti kehilangan data, kerusakan pada sistem *server*, menurunnya kualitas layanan bagi pengguna, hingga berpotensi mengakibatkan hilangnya aset penting milik institusi (Purnama et al., 2023). Sistem Keamanan Jaringan merupakan sebuah upaya yang bertujuan untuk mencegah dan mengidentifikasi adanya pengguna tidak sah (penyusup) dalam suatu lingkungan jaringan. Tindakan pencegahan ini berfungsi untuk menghentikan akses penyusup terhadap segala informasi atau sumber daya di dalam jaringan yang telah mereka coba susupi. Sistem Keamanan Jaringan juga menjadi elemen penting dalam menjaga stabilitas jaringan serta memastikan keefektifan pengelolaan data pengguna (Rivaldi & Marpaung, 2023).

Intrusion Detection System (IDS) dapat didefinisikan sebagai perangkat, teknik, atau sumber daya yang berfungsi untuk mendeteksi dan melaporkan

aktivitas yang terjadi dalam jaringan komputer (Ramadhan et al., 2024). berfungsi sebagai sistem peringatan dini yang mendeteksi adanya serangan pada jaringan komputer. Saat sebuah serangan terdeteksi, IDS akan segera menginformasikan hal tersebut kepada *administrator* jaringan agar dapat diambil tindakan pencegahan. Selain itu, IDS juga mencatat seluruh aktivitas yang mencurigakan maupun upaya yang berpotensi mengganggu kestabilan jaringan komputer, termasuk berbagai jenis serangan yang terjadi. Penelitian ini bertujuan untuk menerapkan IDS dalam sistem jaringan dan menganalisis data *log* yang dihasilkan guna mengidentifikasi tipe dan karakteristik serangan yang masuk. Analisis mendalam terhadap *log* dari IDS ini diharapkan dapat menjadi dasar dalam memperkuat sistem keamanan jaringan komputer (Widodo & Aji, 2022).

Intrusion Prevention System (IPS) merupakan sebuah sistem yang berperan dalam menolak paket data terindetifikasi sebagai potensi serangan dan memberikan peringatan terkait ancaman tersebut (Zulmy Alhamri et al., 2023). IPS dirancang untuk mendeteksi dan mencegah serangan dengan memonitor lalu lintas jaringan secara *real-time*. IPS berfungsi dengan menganalisis paket data yang masuk dan keluar dari jaringan, serta menerapkan kebijakan keamanan untuk memblokir atau mengizinkan akses berdasarkan aturan yang telah ditentukan. Metode ini tidak hanya mendeteksi serangan, tetapi juga dapat mengambil tindakan otomatis untuk mencegah akses yang tidak sah, seperti memblokir alamat IP yang mencurigakan atau menutup *port* yang terancam (Syaiful Huda & Subektiningsih, 2024).

Snort yaitu sistem deteksi dan pencegahan intrusi (IDS/IPS) *open-source* yang menerapkan pendekatan berbasis *signature* dan analisis protokol untuk

mengidentifikasi serangan jaringan. *Snort* berperan sebagai alat yang digunakan untuk mendeteksi sekaligus mencegah ancaman, terutama ketika paket data dalam lalu lintas jaringan teridentifikasi sebagai potensi serangan. Di dalam *Snort*, terdapat aturan-aturan khusus yang berfungsi layaknya *firewall*, yang bertugas memantau dan memeriksa setiap aliran data yang melintas di dalam jaringan. Aplikasi *Snort* ini berjalan berdasarkan kumpulan aturan (*rule set*) dengan format tertentu, yang memungkinkan sistem *Linux* untuk mengenali pola-pola serangan yang dilakukan oleh penyerang. Apabila ditemukan aktivitas yang mencurigakan atau perilaku tidak normal, *Snort* akan segera memberikan notifikasi peringatan kepada *administrator* (Ramadhan et al., 2024).

IPTables merupakan utilitas *firewall* berbasis *command-line* pada sistem *Linux* yang berfungsi sebagai framework packet filtering yang memungkinkan sistem *administrator* mengonfigurasi aturan keamanan jaringan melalui struktur *chains* dan *tables*. *IPTables* juga berfungsi untuk menyaring paket data yang masuk, keluar, maupun yang diteruskan, dengan kriteria tertentu seperti alamat IP, identitas jaringan, nomor *port*, sumber asal, tujuan, jenis protokol yang digunakan, hingga tipe koneksi dari setiap paket data yang diproses sesuai kebutuhan (Barends et al., 2022).

Pada penelitian yang pernah dilakukan oleh Hasri Awal, Aggy Pramana Gusman pada tahun 2023. Dengan judul Implementasi Intrusion Detection Prevention System Sebagai Sistem Keamanan Jaringan Komputer Kejaksaan Negeri Pariaman Menggunakan *Snort* dan *IPTables* Berbasis *Linux*. Penelitian ini menjelaskan implementasi metode *Intrusion Detection Prevention System* (IDPS) menggunakan *Snort* dan *IPTables* pada jaringan komputer di Kejaksaan Negeri

Pariaman, bertujuan untuk memberikan keamanan dalam sebuah sistem jaringan komputer untuk menghindari serangan dan melindungi jaringan komputer, maka perlu adanya keamanan jaringan dari serangan seperti *Denial of Service* (DoS) dan *port scanning*. Metodologi yang digunakan melibatkan instalasi *Snort* sebagai sistem deteksi intrusi yang memberikan *alert* secara *real-time* terhadap aktivitas mencurigakan, serta *IPTables* sebagai sistem pencegahan intrusi yang memblokir alamat *IP intruder*. Hasil penelitian menunjukkan bahwa *Snort* berhasil mendeteksi serangan dan memberikan peringatan, sementara *IPTables* efektif dalam menghentikan serangan dengan memblokir *intruder*. Selain itu, pengujian kualitas layanan *server* menunjukkan peningkatan indeks dari 2 menjadi 3,75 setelah penerapan IDPS, yang menandakan perbaikan signifikan dalam kualitas layanan jaringan (Awal, 2023).

Dari permasalahan diatas maka diusulkan menggunakan metode *Intrusion Detection and Prevention System* (IDPS) menggunakan *Snort* dan *IPTables* berbasis *Linux* bertujuan untuk meningkatkan keamanan jaringan dari ancaman *cyber*. *Snort* berfungsi sebagai *Intrusion Detection System* (IDS) yang menganalisis lalu lintas jaringan secara *real-time*, mendeteksi pola serangan berdasarkan *signature* atau perilaku mencurigakan, dan mencatat aktivitas yang mencurigakan. Selain itu, *Snort* juga dapat dikonfigurasi sebagai *Intrusion Prevention System* (IPS) untuk secara otomatis memblokir ancaman yang teridentifikasi. *IPTables*, sebagai *firewall* bawaan *Linux*, digunakan untuk mengatur aturan lalu lintas jaringan, mencegah akses tidak sah, serta memperkuat mekanisme pencegahan serangan. Kombinasi *Snort* dan *IPTables* memungkinkan sistem untuk mendeteksi, mencatat, serta secara aktif mencegah berbagai ancaman siber seperti

serangan *DDoS*, *brute force*, serta akses ilegal terhadap sistem sehingga menjaga keandalan serta keamanan data yang dikelola.

Dari permasalahan tersebut penulis ingin mengangkat judul penelitian yaitu "**IMPLEMENTASI SISTEM KEAMANAN JARINGAN DENGAN METODE INTRUSION DETECTION DAN PREVENTION SYSTEM (IDPS) PADA KANTOR CAMAT LUBUK BEGALUNG MENGGUNAKAN SNORT DAN IPTABLES BERBASIS LINUX".**

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah telah diuraikan di atas dapat disimpulkan permasalahan yang akan dibahas pada laporan ini sebagai berikut:

1. Bagaimana penerapan metode *Intrusion Detection dan Prevention System* (IDPS) dapat meningkatkan keamanan jaringan di Kantor Camat Lubuk Begalung?
2. Bagaimana cara kerja *Snort* sebagai sistem deteksi intrusi dalam mendeteksi dan menganalisis serangan jaringan?
3. Bagaimana *IPTables* dapat digunakan untuk mencegah serangan yang terdeteksi oleh *Snort*?

1.3 Hipotesa

Hipotesa merupakan dugaan sementara dimana nantinya akan dibuktikan dengan hasil penelitian yang dilakukan. Berdasarkan permasalahan yang ada dapat dikemukakan beberapa hipotesa sebagai berikut:

1. Diharapkan penelitian implementasi sistem *Intrusion Detection* dan *Prevention System* (IDPS) menggunakan *Snort* dan *IPTables* yang

dilakukan dapat memberi secara signifikan mengurangi jumlah serangan yang berhasil masuk ke jaringan Kantor Camat Lubuk Begalung.

2. Diharapkan dengan penggunaan *Snort* sebagai sistem deteksi intrusi akan meningkatkan kemampuan Kantor Camat Lubuk Begalung dalam mendeteksi dan merespons ancaman keamanan jaringan secara *real- time*.
3. Diharapkan dengan konfigurasi *IPTables* yang tepat, berdasarkan informasi yang diberikan oleh *Snort*, akan meningkatkan efektivitas pencegahan serangan dan mengurangi risiko akses tidak sah ke jaringan.

1.4 Batasan Masalah

Untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah dalam penyusunan penelitian ini maka peneliti memberikan batasan masalah yaitu:

1. Implementasi IDPS hanya menggunakan *Snort* sebagai sistem deteksi/pencegahan intrusi dan *IPTables* sebagai *firewall*, tanpa melibatkan sistem keamanan lainnya.
2. Sistem IDPS yang diimplementasikan akan berbasis pada sistem operasi *Kali Linux*, dengan penggunaan *Snort* sebagai alat deteksi intrusi dan *IPTables* sebagai alat pencegahan, tanpa mempertimbangkan alat atau teknologi lain.
3. Objek Penelitian dilakukan khusus pada jaringan internal Kantor Camat Lubuk Begalung, tanpa melibatkan jaringan eksternal atau *cloud computing*.

1.5 Tujuan Penelitian

Dalam melaksanakan penelitian ini tujuan yang ingin dicapai diantaranya yaitu:

1. Menerapkan sistem *Intrusion Detection and Prevention System* (IDPS) sehingga dapat memberikan sistem keamanan jaringan di Kantor Camat Lubuk Begalung.
2. Mengetahui cara kerja penggunaan *Snort* sebagai sistem deteksi intrusi dalam mendeteksi dan menganalisis serangan jaringan sehingga dapat diketahui tingkat sistem keamanan jaringan tersebut.
3. Mengetahui cara kerja penggunaan *IPTables* dalam mencegah serangan yang terdektesi oleh *Snort*.

1.6 Manfaat Penelitian

Manfaat dari penelitian ini yaitu:

1. Dengan mengimplementasikan sistem *Intrusion Detection and Prevention System* (IDPS) menggunakan *Snort* dan *IPTables* untuk meningkatkan keamanan jaringan Kantor Camat Lubuk Begalung.
2. Dengan mengukur efektivitas sistem *Intrusion Detection and Prevention System* (IDPS) menggunakan *Snort* dan *IPTables* untuk mendeteksi dan mencegah berbagai jenis serangan yang terjadi.
3. Bermanfaat untuk memberikan rekomendasi dan panduan bagi pengelola jaringan di Kantor Camat Lubuk Begalung mengenai praktik dalam pemeliharaan dan pengelolaan sistem *Intrusion Detection and Prevention System* (IDPS), termasuk langkah-langkah yang perlu diambil untuk menjaga sistem.

1.7 Gambaran Umum Objek Penelitian

Penelitian ini dilakukan pada Kantor Camat Lubuk Begalung, yang merupakan salah satu instansi pemerintahan di bawah naungan Pemerintah Kota Padang. Kantor ini memiliki peran penting dalam memberikan pelayanan administrasi kependudukan, pemerintahan, dan kemasyarakatan kepada masyarakat di wilayah kecamatan tersebut. Seiring dengan meningkatnya kebutuhan pelayanan berbasis digital, kantor ini telah mengimplementasikan jaringan komputer untuk menunjang aktivitas operasional sehari-hari. Namun, penggunaan jaringan komputer juga berpotensi menimbulkan ancaman keamanan seperti serangan siber dan akses tidak sah. Oleh karena itu, objek penelitian ini dipilih untuk mengkaji bagaimana penerapan sistem keamanan jaringan yang tepat, khususnya melalui metode *Intrusion Detection and Prevention System* (IDPS), guna meningkatkan perlindungan terhadap data dan infrastruktur jaringan yang dimiliki.

1.7.1 Sekilas Tentang Kantor Camat Lubuk Begalung

Kantor Camat Lubuk Begalung merupakan salah satu instansi pemerintahan di Kota Padang, Sumatera Barat, yang bertanggung jawab atas pelayanan administratif dan pemerintahan di Kecamatan Lubuk Begalung. Kecamatan ini merupakan salah satu kecamatan terbesar di Kota Padang dengan jumlah penduduk yang cukup padat dan wilayah yang mencakup berbagai aspek kehidupan, mulai dari pemukiman, perdagangan, hingga sektor pendidikan. Sebagai pusat pemerintahan kecamatan, kantor camat memiliki peran penting dalam mengelola berbagai aspek administrasi dan pelayanan publik, termasuk pengurusan dokumen kependudukan, perizinan, dan program-program pembangunan daerah. Dengan lokasi strategis, kantor ini melayani masyarakat yang tinggal di wilayah Lubuk Begalung dan sekitarnya.

Kantor Camat Lubuk Begalung yang beralamat di Blok S No., Jl. Berlian Raya No.2, Pagambiran Ampalu Nan XX, Kec. Lubuk Begalung, Kota Padang, Sumatera Barat. Jam operasional Kantor Camat Lubuk Begalung ini yaitu buka pada hari Senin sampai Jumat, dari pukul 08.00 pagi hingga pukul 16.00 WIB.

Kantor Camat Lubuk Begalung merupakan pusat pelayanan masyarakat yang berkomitmen untuk memberikan layanan yang cepat dan efisien. Dalam menjalankan tugasnya, kantor ini berkoordinasi dengan berbagai instansi terkait untuk memastikan bahwa kebutuhan masyarakat terpenuhi. Selain itu, kantor ini juga berperan dalam menjaga keamanan dan ketertiban di wilayahnya. Melalui berbagai kegiatan, seperti sosialisasi dan kerja sama dengan pihak kepolisian, kantor ini berupaya menciptakan lingkungan yang aman dan nyaman bagi warganya. Dengan demikian, Kantor Camat Lubuk Begalung tidak hanya berfungsi sebagai penyedia layanan, tetapi juga sebagai penggerak pembangunan dan pemberdayaan masyarakat di kecamatan tersebut.

1.7.2 Visi dan Misi Kantor Camat Lubuk Begalung

1. Visi:

   Menjadi Kecamatan Terbaik dalam Melayani Masyarakat untuk Mendorong Terciptanya Masyarakat yang Sejahtera, Religius dan Berbudaya.

2. Misi:

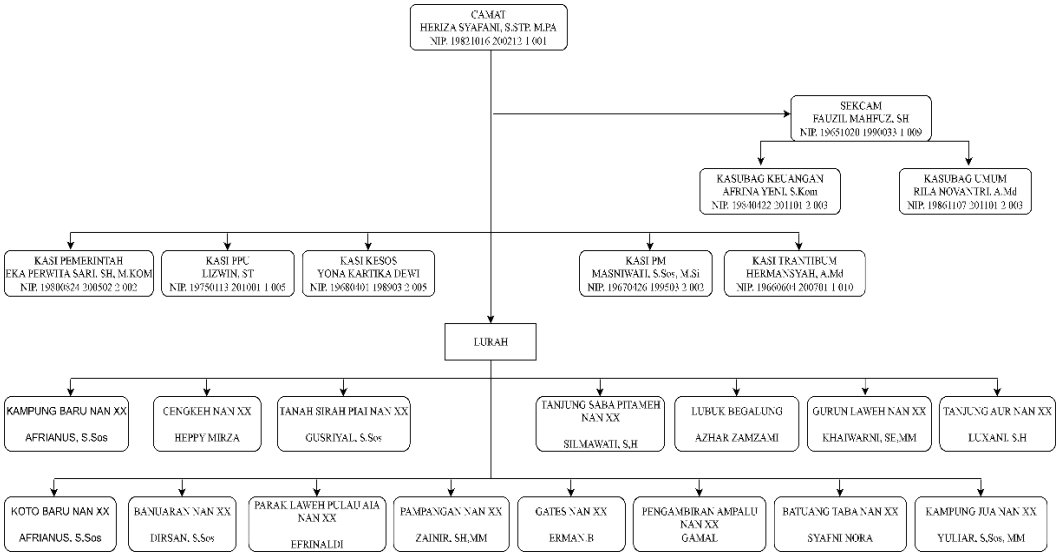
   1. Memberikan pelayanan administrasi pemerintahan, pembangunan dan sosial kemasyarakatan secara cepat, akurat dan transparan, koordinatif dan akuntabel.
   2. Melaksanakan pelimpahan tugas dan wewenang dari Walikota dalam penyelenggaran tugas umum pemerintahan secara baik, profesional dan

akuntabilitas untuk mendorong terciptanya kesejahteraan masyarakat dalam suasana religious dan berbudaya.

3. Menciptakan ketentraman dan ketertiban umum melalui peningkatan koordinasi dengan penegakkan peraturan dan perundang-undangan.

1.7.3 Struktur Organisasi Kantor Camat Lubuk Begalung

Dengan adanya struktur organisasi diharapkan akan dapat diketahui dengan jelas mengenai tugas, wewenang, dan tanggung jawab di Kantor Camat Lubuk Begalung. Adapun Struktur Organisasi dapat Kantor Camat Lubuk Begalung dilihat pada Gambar 1.1 sebagai berikut:



Sumber: Kantor Camat Lubuk Begalung, April 2025

Gambar 1.1 Struktur Organisasi Kantor Camat Lubuk Begalung