BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi semakin berkembang dengan cepat, teknologi informasi sudah menjadi kebutuhan suatu instansi. Seiring perkembangan jaringan peningkatan layanan yang cepat dan efisien harus selalu diperhatikan,dengan jaringan terstruktur dapat mempermudah dalam melakukan pengaksesan dan perawatan jaringan (Fauzi et al., 2023).

Penenlitian yang dilakukan oleh (Syani, 2020) dengan judul Implementasi Intrusion Detection System (IDS) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Server (VPS). Menjelaskan tentang teknologi virtual private server (VPS) khususnya yang menggunakan system operasi linux Debian, semakin dimudahkan dengan adaya layanan dari beberapa penyedia VPS baik lokal mapun non lokal, tetapi terdapat masalah kerentanan apabila, para pengelola server tidak Malukan pengujian terlebih dahulu terhadap ketahanan serangan dari pihak luar, dengan metode Network Development life Cycle (NDLC) salah yang paling popular dalam tahapan Monitoring yaitu menggunakan software Intrusion Detection System (IDS) Suricata. Suricata mampu menampilkan log - log dari hasil aktivitas yang mencurigakan secara detail dengan waktu, tanggal dan alamat IP yang melakukan aktivitas tersebut bahkan dengan tools yang digunakan untuk melakukan aktivitas tersebut. Selain itu juga suricata bisa mendeteksi jika ada aktivitas mencurigakan

yang berhubungan dengan jaringan.

Penelitian yang dilakukan oleh (Pitriyanti et al., 2023) dengan judul Prototype Sistem Deteksi Serangan Pada Server Samsat Menggunakan Intrusion Detection System (IDS) Berbasis Snort. Penelitian ini menjelaskan tentang Kantor Sistem Administrasi Satu Atap atau yang lebih dikenal dengan Samsat Empat di Kabupaten Lawang merupakan sebuah instansi pemerintah yang menyelenggarakan pajak jalan raya yang transparan dan transparan kepada masyarakat. Permasalahan di kantor samsat kabupaten empat lawang adalah server samsat tidak terlindungi dari serangan pihak - pihak yang tidak bertanggung jawab yang dapat menyebabkan kerusakan samsat di kabupaten empat lawang, baik itu kehilangan data atau kemudian data rusak. Berdasarkan hal tersebut diperlukan suatu sistem untuk mendeteksi serangan pada server Samsat Kabupaten Empat Lawang untuk mencegah serangan dari pihak yang tidak bertanggung jawab dan mengamankan server Samsat dengan IDS (Intrusion Detection System) dengan Snort untuk mendeteksi serangan.

Penelitian yang dilakukan oleh (Fauzi et al., 2023) dengan judul Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS) menjelaskan tentang A Madrasah Aliyah Negeri Purwakarta. adalah sekolah menengah atas negeri yang berada di wilayah Kabupaten Purwakarta Kecamatan Purwakarta,semua aktivitas disekolah ini sudah menggunakan jaringan komputer untuk mendukung sarana kegiatan yang ada disekolah ini.sehingga jaringan komputer menjadi kebutuhan utama di Madrasalah Aliyah Negeri Purwakarta dalam menjalankan segala aktivitasnya, jaringan komputer di Madrasah Aliyah Negeri Purwakarta. pada saat ini

belum menerapkan system kemanan jaringan komputer, karena tidak adanya system keamanan jaringan komputer yang diterapkan di Madrasah Aliyah Negeri Purwakarta,masih rentan terkena serangan diantaranya Ping Attack, Network Scanning dan DDOS. Hasil dari penilitian ini adalah suatu rancangan system keamanan jaringan komputer berbasis Intrusion Detection System (IDS) menggunakan snort dan portsentry untuk mendeteksi adanya sebuah serangan yang masuk ke dalam jaringan komputer Madrasah Aliyah Negeri Purwakarta seperti Ping icmp,nmap (port scan) dan DDOS, dengan mendapatkan sebuah notifikasi serangan yang masuk ke jaringan komputerm, serangan tersebut dapat dicegah dengan menerapkan portsentry sehingga serangan seperti Ping icmp,nmap dan DDOS tidak akan bisa masuk ke dalam jaringan komputer. Penelitian yang dilakukan oleh (Alamsyah et al., 2020) dengan judul Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. Penelitian ini menjelaskan tentang penyusup yang dapat melakukan port scanning, masuk pada sistem menggunakan port-port yang terbuka seperti telnet, ftp dan lainnya. Tujuan dari penelitian ini adalah mengimplementasikan IDPS, mampu mendeteksi dan memblokir adanya serangan dari penyusup. Untuk melakukan kemananan jaringan dari berbagai ancaman serangan dibutuhkan sebuah sistem yang dapat mendeteksi dan mencegah secara langsung. Metode yang dapat digunakan yaitu Intrusion Detection and Prevention System (NIDPS). NIDPS dapat mendeteksi dan melakukan blokir terhadap serangan yang terjadi. Sistem keamanan ini dikolaborasikan dengan IP Tables. IP Tables ini berfungsi untuk memfilter paket data yang masuk dan mendrop paket data yang terindikasi serangan. Dengan adanya Intrusion Detection

and Prevention system ini dapat mendeteksi adanya serangan dan melakukan pencegahan dengan cara memblokir paket data yang dikirim oleh penyusup melalui port scanning, serangan ftp, dan telnet.

Dinas Kominfo Padang merupakan Badan Usaha Milik Negara (BUMN) yang bergerak Di bidang jasa layanan tatanan pemerintahan yang baik, bersih, dan profesional dan teknologi informasi dan komunikasi (TIK). Beralamat di Jl. Bagindo Azis Chan No. 1 Aie Pacah - Kota Padang Sumatera Barat. Kantor ini merupakan kantor Dinas wilayah sumatera barat. Keamanan pada Dinas Kominfo Padang sangat penting, dan harus diperhatikan dalam jaringan komputer. Sistem keamanan ini dapat berupa pendeteksi dan pencegahan terjadinya serangan yang di lakukan oleh penyusup. Kendala yang ada pada kantor dalam hal keamanan jaringan, dimana dalam file log sering kali terdapat ip address atau identitas penyusup yang mencoba mengambil kendali server menggunakan akses root ke server pusat database perusahaan. Tujuan dari penelitian ini adalah untuk menjaga kemanan sebuah sistem yang dapat meminimalisasi serangan-serangan terhadap jaringan bahkan server dari penyusup ini. Diharapkan dapat mendeteksi dan mengidentifikasikan paket yang keluar masuk ke jaringan. Alat deteksi sangat diperlukan dalam kondisi ini, yang dapat mendeteksi terjadinya intrusi pada sistem server jaringan. Alat deteksi yang dimaksud adalah Intrusion Detection System (IDS). Knowledge-based (signature-based) IDS dapat mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan database rule IDS (berisi signature - signature paket serangan). Metode yang dapat digunakan yaitu Network Intrusion Detection System (NIDS). Jika paket data tersebut sama sekali tidak mempunyai pola yang

sama dengan pola di database 4 rule IDS, maka paket data tersebut dianggap bukan serangan. Kemudian IDS engine akan membaca alert dari IDS (antara lain berupa jenis serangan dan IP address penyusup) untuk kemudian memerintahkan firewall untuk memblok akses koneksi ke sistem dari penyusup tersebut**.** IDS (Intrution Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. (Agustin et al., 2019).

Dari permasalahan tersebut penulis ingin mengangkat judul penelitian yaitu : "**ANALISA KEAMANAN JARINGAN PADA DINAS KOMINFO PADANG MENGGUNAKAN INTRUSION DETECTION SYSTEM DENGAN METODE SIGNATURE-BASED DAN PENCEGAHANNYA BERBASIS FIREWALL**"

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka dapat dirumuskan beberapa rumusan masalah yaitu :

1. Bagaimana analisa keamanan jaringan di dinas kominfo padang dengan metode signature-based dan pencegahannya berbasis firewall?
2. Bagaimana menggunakan intrusion detection system dengan metode signature-based dan firewall dalam membangun keamanan jaringan di dinas kominfo padang?
3. Bagaimana sistem keamanan jaringan mendeteksi dan mencegah serangan dari penyusup di dinas kominfo padang?

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. Dengan analisa keamanan jaringan menggunakan ids signature-based dan pencegahannya berbasis firewall ini dapat menunjukkan hasil yang baik bagi dinas kominfo padang.
2. Dengan menggunakan ids signature-based dan firewall dapat membangun keamanan jaringan di dinas kominfo padang dalam keamanan data dari kemungkinan penyusup.
3. Dengan sistem keamanan jaringan menggunakan ids metode signature-based dan firewall dapat mencegah dan mengatasi serangan penyusup di dinas kominfo padang.

1.4 Batasan Masalah

Menghindari terlalu luasnya permasalahan dan pemecahan masalah yang dilajukan, maka perlu dibatasi sistem yang dirancang. Batasan-batasan yang diberikan adalah :

1. Menganalisa sistem keamanan jaringan intrusion detection system dengan metode signature-based untuk mencegah penyusup dan firewall untuk memblok yang tidak bertanggung jawab.
2. Mendeteksi dan mengedentifikasi menggunakan ids setiap paket yang keluar masuk ke jaringan.

3. Menguji firewall dalam pencegahan penyusup menggunakan block ip address.

1.5 Tujuan Penelitian

Dalam melaksanakan penelitian ini terdapat tujuan yang ingun dicapai, adapun diantaranya adalah :

1. Menganalisa keamanan jaringan intrusion detection system dengan metode signature-based dan pencegahan menggunakan firewall.
2. Untuk mendeteksi dan mengidentifikasi ids setiap paket yang masuk dan keluar ke jaringan kantor kominfo padang.
3. Untuk menguji performa dalam pencegahan penyusup menggunakan firewall.

1.6 Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Bagi penulis berkenaan dengan pekerjaan penulis sebagai mahasiswa Teknik Informatika dengan kosentrasi studi network engineering, manfaat dari penelitian tugas akhir ini adalah dapat mengetahui sejauh mana keamanan jaringan menggunakan ids signature-based dan pencegahannya dengan firewall.
2. Bagi pihak lain sebagai informasi/referensi bagi para peneliti yang akan melakukan penelitian yang berhubungan dengan ids khususnya signature-based dan firewall ataupun membantu orang lain yang membutuhkan informasi tentang keamanan jaringan menggunakan ids dengan metode signature-based dan pencegahaannya dengan firewall.

1.7 Gambaran Umum Objek Penelitian

Dinas Komunikasi dan Informatika (Diskominfo) Kota Padang dibentuk berdasarkan Peraturan Daerah Kota Padang Nomor 9 Tahun 2016 tentang Pembentukan dan Penyusunan Perangkat Daerah di Lingkungan Pemerintah Kota Padang. Dalam rangka melaksanakan kewenangan di bidang Komunikasi dan Informatika, maka berdasarkan Peraturan Walikota Nomor 40 Tahun 2016, ditetapkanlah tugas pokok dan fungsi Dinas Komunikasi dan Informatika Kota Padang. Dinas Komunikasi dan Informatika (Diskominfo) Kota Padang Panjang sebagai salah satu Satuan Kerja Perangkat Daerah (SKPD) di Kota Padang. Pada awalnya Dinas Komunikasi Dan Informasi Kota Padang ini bernama Dinas Hubungan Komunikasi Dan Informasi (Dishubkominfo) yang masih bergabung dengan Dinas Perhubungan pada tahun 2011 sampai akhir tahun 2016 dan pada 1 Januari 2017 Diskominfo sudah berdiri sendiri menjadi Dinas. Ketika masih bernama Dishubkominfo tugasnya adalah mengatur dan memberikan izin untuk akses Jaringan, warnet, mendirikan Radio dan Televisi Kabel. Namun, setelah berdirinya Diskominfo semua tugas tersebut menjadi wewenang Pemerintah Pusat. Setelah berdiri , Diskominfo mempunyai 2 bidang yaitu Bidang Informasi dan Komunikasi Publik (IKP) dan Bidang E-Government dan Teknologi Informasi. Secara umum tugas dari IKP sendiri yaitu untuk Penyebarluasan Informasi Publik dan E-Gov Layanan Aplikasi Terintegrasi dan memberikan layanan akses internet.

1.7.1 Sekilas Tentang Dinas Kominfo Padang

Dinas Kominfo Padang merupakan Kantor Badan Usaha Milik Negara (BUMN) yang bergerak di bidang jasa layanan tatanan pemerintahan yang baik,

bersih, dan profesional dan teknologi informasi dan komunikasi (TIK). Beralamat di Jl. Bagindo Azis Chan No. 1 Aie Pacah - Kota Padang Sumatera Barat. Kantor ini merupakan kantor dinas kominfo wilayah sumatera barat. Untuk Untuk nomor telepon yang dapat dihubungi (0751) 4640800. Dan jam operasional pada Dinas Kominfo Padang yaitu buka hari senin sampai jumat, serta melayani pelanggan dari pukul 08.00 pagi hingga pukul 16.00 sore.

1.7.2 Visi & Misi DinasKominfo Padang

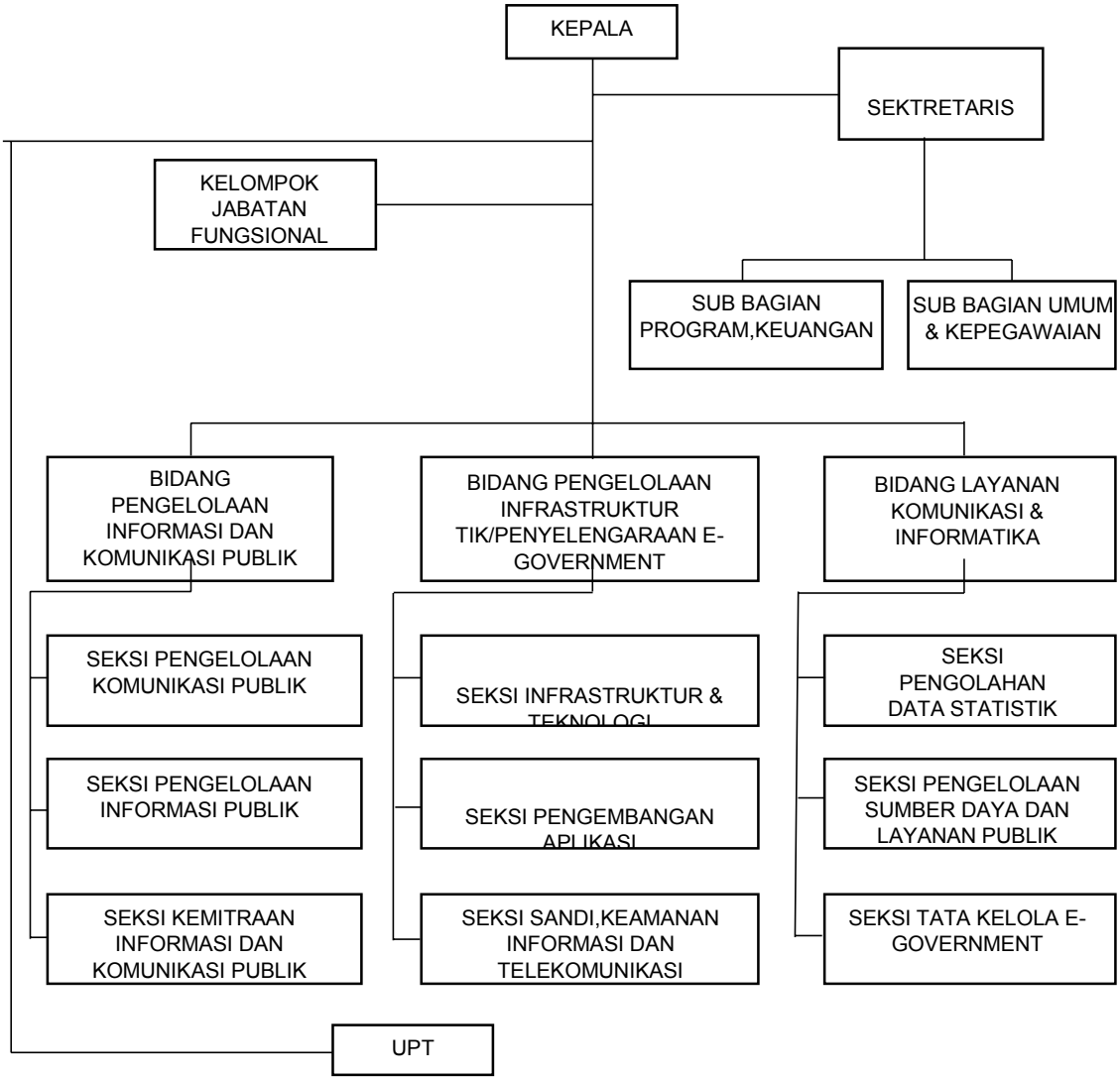
Visi

Terwujudnya Sumatera Barat yang Unggul dan Berkelanjutan.

Misi

1. Meningkatkan kualitas sumber daya manusia yang sehat, berpengetahuan, terampil dan berdaya saing.
2. Meningkatkan tata kehidupan sosial kemasyarakatan berdasarkan Falsafah Adaiak Basandi Syara', Syara' Basandi Kitabullah.
3. Meningkatkan usaha perdagangan dan industri kecil/menengah serta ekonomi berbasis digital.
4. Meningkatkan nilai tambah dan produktifitas pertanian, perkebunan, perternakan dan perikanan.

1.7.3 Struktur Organisasi Dinas Kominfo Padang



Sumber : Struktur organisasi dinas kominfo padang

Gambar 1. 1 Struktur Organisasi Dinas Kominfo Padang

1.7.3 Pembagian Tugas dan Tanggung Jawab

Uraian tugasnya diatur dalam Peraturan Gubernur Sumatera Barat Nomor 78 Tahun 2016 tentang Rincian Tugas Pokok Dan Fungsi Organisasi Perangkat Daerah Dinas Komunikasi dan Informatika Provinsi Sumatera Barat. Untuk

menyelenggarakan tugas pokok Dinas Komunikasi dan Informatika Provinsi Sumatera Barat mempunyai fungsi sebagai berikut :

1. Perumusan Kebijakan teknis bidang komunikasi dan informatika, statistik dan persandian.
2. Penyelenggaraan urusan pemerintahan dan pelayanan umum bidang bidang komunikasi dan informatika, statistik dan persandian.
3. Pembinaan dan fasilitasi bidang komunikasi bidang komunikasi dan informatika, statistik dan persandian lingkup Provinsi dan Kabupaten/Kota.
4. Pelaksanaan kesekretariatan Dinas.
5. Pelaksanaan tugas di bidang Pengelolaan Informasi dan Komunikasi Publik, Bidang Pengelolaan Infrastruktur TIK/Penyelenggaraan E-Government, dan Bidang Layanan Komunikasi dan Informatika serta Unit Pelaksana Teknis Daerah dan Fungsional KISS.
6. Pemantauan, evaluasi dan pelaporan di bidang bidang komunikasi dan informatika, statistik dan persandian.
7. Pelaksanaan tugas lain yang diberikan oleh Pimpinan.