BAB 1
PENDAHULUAN

1.1 Latar Belakang

UPTD (Unit Pelaksana Teknis Daerah) Instalasi Farmasi Kabupaten Tangerang adalah unsur penunjang dari sebagian tugas dinas dalam bidang pengelolaan obat, vaksin, dan perbekalan farmasi yang dipimpin oleh kepala UPTD yang bertanggung jawab langsung kepada kepala dinkes kabupaten Tangerang. UPTD. Instalasi Farmasi Kabupaten Tangerang banyak melakukan aktivitas yang berhubungan dengan pertukaran data baik data besar maupun kecil seperti data obat-obatan, data pendistribusian obat dan data pencatatan berbagai alat kesahatan lainnya.

UPTD (Unit Pelaksana Teknis Daerah) Instalasi Farmasi Kabupaten Tangerang membangun sebuah website bernama e-logistik Digifarma yang dipergunakan untuk melakukan pengolahan data, dan untuk mengakses website tersebut UPTD. Instalasi Farmasi Kabupaten Tangerang membuat dua akses yaitu melalui website Aplikasi Kabupaten Tangerang dan direct link yang langsung menuju halaman login webiste tersebut. UPTD. Instalasi Farmasi Kabupaten Tangerang hanya dapat mengakses website tersebut melalui alamt ip statis yang terkoneksi dengan internet. Berdasarkan Hasil Wawancara kepada staff Farmasi UPTD.Instalasi Farmasi Kabupaten Tangerang Bapak Ubaedillah,S.Farm , pernah terjadi pengelabuan (phishing) pada sistem UPTD.Instalasi Farmasi Kabupaten Tangerang, hal tersebut sudah terjadi sebanyak dua kali yang menyebabkan data data hilang dan sistem harus di install ulang. Phishing merupakan tindakan pencurian informasi menggunakan entitas elekronik seperti website [1]. Selain phising, seringkali terjadi gangguan seperti, akses pada website yang sangat berat, website yang tidak dapat di akses dan terkadang tidak dapat memasukkan data ke website, yang disebabkan komputer yang terkoneksi pada jaringan tidak terjamin bebas dari virus, malware dan semacamnya. Berdasarkan indikasi-indikasi tersebut terdapat kemungkinan jika komputer yang digunakan terkena virus ataupun malware. Malware merupakan perangkat lunak yang dirancang untuk merusak atau

menggangu komputer, sistem komputer, atau jaringan. Malware mengacu pada program yang disisipikan secara teselubung dengan tujuan untuk melihat informasi korban baik berbentuk data, aplikasi ataupun sistem operasi [2] [3]. Penyisipan malware bisa terjadi karena beberapa kemungkinan, seperti kesalahan pengguna yang tidak sengaja mengakses website yang berisi malware, tidak adanya antivirus pada komputer yang digunakan dan sebagainya. Apabila terjadi gangguan pada website maka penginputan data farmasi akan terganggu dan berakibat keterlambatan pelaporan dan akan sangat berbahaya jika data yang terdapat pada wabsite menjadi rusak. Untuk menjaga sistem dari kerentanan keamanan tersebut diperlukan peningkatan keamanan sistem dari luar maupun dari dalam yang dapat memantau dan melakukan pencegahan dini terhadap penyusupan atau kejadian yang dapat membuat sistem jaringan menjadi berjalan tidak seperti sebagaimana mestinya.

Salah satu metode yang dapat digunakan untuk mengatasi serangan-serangan pada jaringan tersebut dapat dilakukan dengan menggunakan metode Intrusion Detection and Prevention System (IDPS). Penerapan Intrusion Detection and Prevention System (IDPS) merupakan salah satu solusi yang dapat digunakan untuk membantu admin dalam memantau dan menganalisa paket-paket berbahaya yang terdapat dalam sebuah jaringan [4]. Intrusion Detection and Prevention System (IDPS) juga dapat melakukan tindakan seperti mengirim alarm , menjatuhkan paket berbahaya yang terdeteksi, mengatur ulang koneksi atau memblokir lalu lintas dari alamat IP yang dicurigai [5]. Snort merupakan Intrusion Detection System (IDS) berbasis open-source yang menggunakan rules sebagai teks untuk mengisntruksi dan memberi aksi terhadapat event yang terdeteksi [6]. Snort dioperasikan menggunakan command lines. Rules Snort terbilang mudah diterapkan namun sangat ampuh untuk mendeteksi setiap intrusi yang mencurigakan [7]. Snort memiliki fitur-fitur yang dapat membantu aktivitas penggunanya seperti dapat berjalan di semua sistem operasi, kemampuan dalam memeriksa protokol dan versi GUI untuk mempermudah monitoring.

PfSense merupakan salah satu Intrusion Prevention System (IPS) yang dapat berkesinambungan dengan snort. PfSense merupakan open-source yang secara

khusus dairancang untuk digunakan sebagai firewall dan router yang sepenuhnya dikelola melalui antarmuka web [8]. PfSense memiliki fitur-fitur yang dapat meningkatkan keamanan pada jaringan seperti menyaring paket data pada TCP dan MAC address dan membatasi traffic.

Berdasarkan permasalahan yang ada peneliti menyimpulkan bahwa diperlukan peningkatan keamanan jaringan dengan cara mengimplementasikan Hybrid Intrusion Detection Prevention System (IDPS) Snort dan pfSense untuk menangani penyerangan berdasarkan alert yang telah dicatat pada log serangan dan juga memberikan log serangan yang baru ke email admin sebagai penunjang keamanan jaringan.

1.2 Identifikasi Masalah

Dari beberapa uraian yang dikemukakan pada latar belakang, maka dapat diidentifikasi masalah-masalah sebagai berikut :

1. Sistem keamanan jaringan yang ada pada UPTD. Instalasi Farmasi Kabupaten Tangerang masih belum sepenuhnya dapat memberikan keamanaan karena belum adanya sistem yang dapat memantau dan menganalisa paket-paket berbahaya.
2. Masih minimnya pengecekan lalu lintas jaringan baik dari luar dan dalam.

1.3 Rumusan Masalah

Dari beberapa uraian yang penulis kemukakan pada bagian latar belakang tersebut, penulis dapat merumuskan permasalahannya sebagai berikut :

1. Bagaimana mencegah dan meminimalisir penyerangan terhadap jaringan pada UPTD.Instalasi Farmasi Kabupaten Tangerang ?
2. Bagaimana Intrusion Detection and Prevention System (IDPS) dengan Snort dan pfSense mendeteksi dan menganalisa setiap intrusi yang terjadi pada lalu lintas jaringan ?

1.4 Maksud dan Tujuan

Berdasarkan rumusan masalah tersebut, maka dapat diketahui maksud dari penelitian ini adalah merancang sistem keamanan dengan metode Intrusion

Detection and Prevention System (IDPS) sebagai peningkatan keamanan pada jaringan UPTD.Instalasi Farmasi Kabupaten Tangerang. Sedangkan tujuan dilakukannya penelitian ini adalah sebagai berikut :

1. Menunjukkan metode Hybrid Intrusion Detection Prevention System (IDPS) dengan Snort dan PfSense dapat digunakan untuk mengamankan jaringan UPTD.Instalasi Farmasi Kab.Tangerang dari serangan jaringan.
2. Merancang sistem keamanan jaringan menggunakan metode Hybrid Intrusion Detection Prevention System (IDPS) dengan Snort dan PfSense untuk mendapat informasi atau laporan serangan jaringan sehingga dapat dipelajari pola serangan yang terjadi dan mengantisipasinya.

1.5 Batasan Masalah

Adapun batasan-batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Jenis IDS yang digunakan adalah Snort.
2. Menggunakan pfSense sebagai Interface dan IPS untuk membaca dan memblokir berdasarkan log serangan.
3. Menggunakan *IP-Address* versi 4.
4. Aktifitas yang dipantau meliputi *malware dan DDoS Attack.*
5. Serangan akan dikelompokan berdasarkan perilaku penyerangan, dimana ada serangan dari luar dan dari dalam.
6. Asal serangan dibedakan berdasarkan Source IP, Source Port dan Klasifiksi serangan.
7. Menggunakan teknik deteksi IDS dengan metode *Signatured-based* dan *Anomaly-based*
8. Serangan pada pengujian ditentukan dan terbatas.
9. Keluaran yang dihasilkan berupa record data penyerangan dalam waktu tertentu.

1.6 Metodologi Penelitian

Penelitian ini akan menggunakan metode analisis deskriptif. Metode analisis deskriptif adalah metode yang berusaha mendeskripsikan suatu gejala, peristiwa, kejadian yang terjadi pada saat sekarang. Metode analisis deskriptif memusatkan perhatian kepada pemecahan masalah-masalah aktual sebagaimana adanya pada saat penelitian dilaksanakan. Metode analisis deskriptif memiliki dua tahap, yaitu tahap pengumpulan data dan pengembangan sistem.

1.6.1 Metode Pengumpulan Data

Metode Pengumpulan data pada penelitian ini dibagi menjadi 2 tahap, yaitu :

1. Studi Literatur

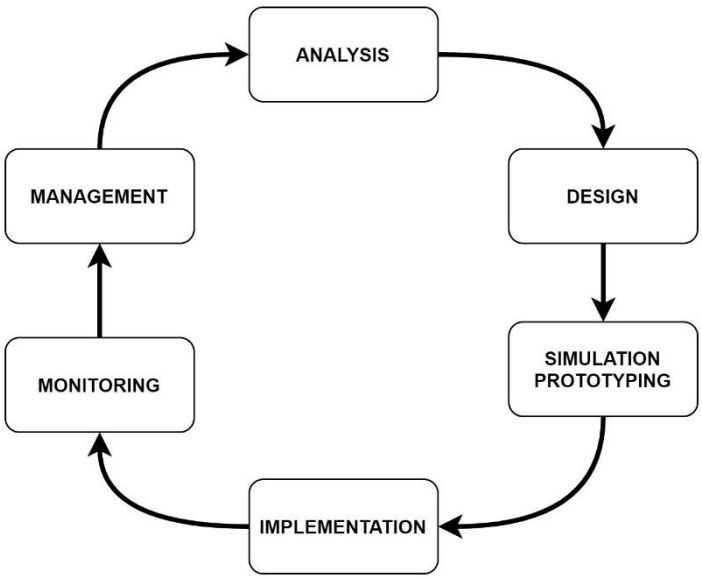
   Studi literatur dilakukan dengan cara mempelajari, meneliti dan menelaah berbagai literatur-literatur mengenai intrusion detection system, signature based, anomaly based, Snort, pfSense, dan jenis serangan/intrusi.

2. Wawancara

   Wawancara merupakan salah satu metode pengumpulan data yang dilakukan dengan tanya jawab secara lisan kepada narasumber utuk mendapatkan informasi yang dibutuhkan. Pada penelitian ini wawancara dilakukan terhadap beberapa staff UPTD.Instalasi Farmasi Kabupaten Tangerang.

1.6.2 Metode Pengembangan Sistem

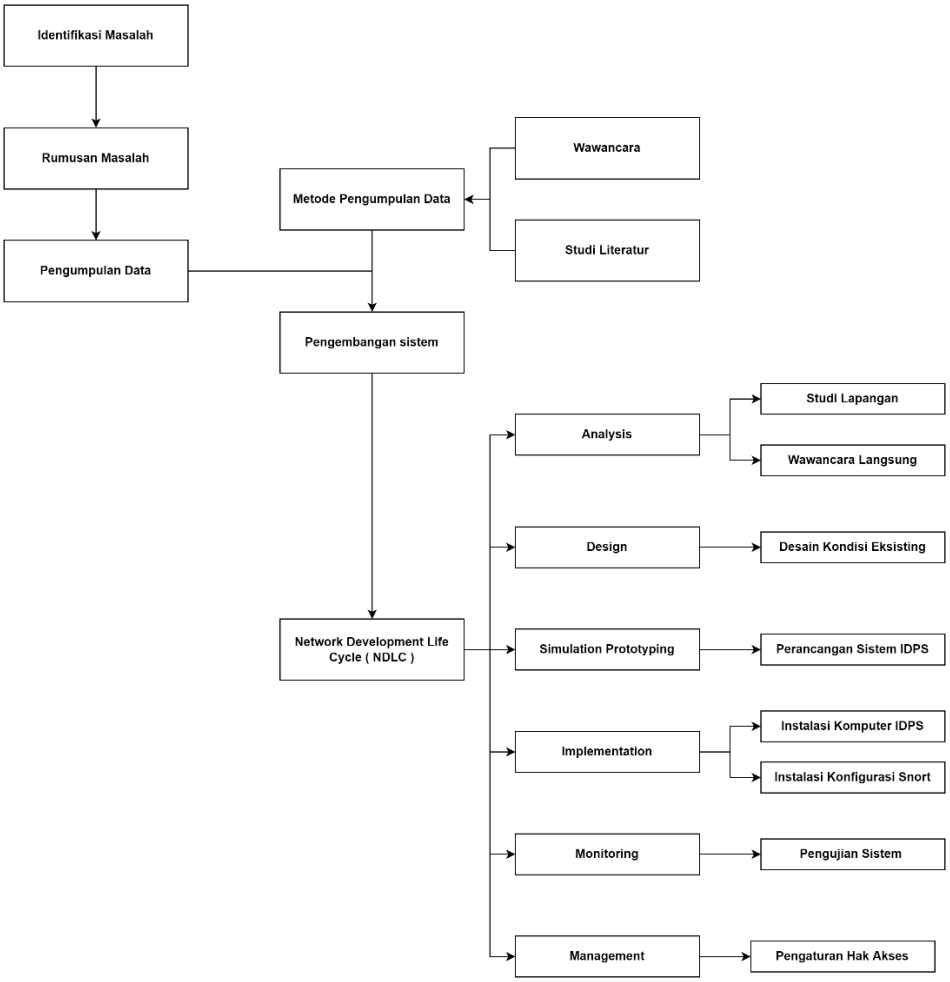
Metode pengembangan sistem yang digunakan adalah metode Network Development Life Cycle (NDLC). NDLC adalah salah satu metode yang dilakukan dalam pengembangan metode dalam jaringan [9]. NDLC memiliki enam tahapan yang dapat dilihat pada Gambar 1.1.



Gambar 1. 1 ***Network Development Life Cycle*** **(NDLC)**

1.6.3 Kerangka Kerja Penelitian

Kerangka kerja penelitian merupakan tahapan yang harus dilalui supaya penelitian dapat berjalan dengan baik dan menghasilkan *output* yang diinginkan. Kerangka kerja pada penelitian ini dapat dilihat pada gambar 1.2.



Gambar 1. 2 Kerangka Kerja Penelitian

1.7 Sistematika Penulisan

Sistematika penulisan disusun untuk memberikan gambaran secara umum mengenai permasalahan dan pemecahannya. Sistematika penulisan skripsi ini adalah sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini membahas mengenai latar belakang, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian, serta sistematika penulisan untuk menjelaskan pokok – pokok pembahasannya.

BAB 2 LANDASAN TEORI

Bab ini akan menjelaskan mengenai objek dari penelitain yaitu keamanan sistem jaringan UPTD Instalasi Farmasi Kabupaten Tangerang, teori – teori pendukung yang berhubungan dengan masalah yang dibahas dan mengenai simulasi serangan yang akan digunakan.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini akan menjelaskan tentang proses analisis sistem dan rancangan umum dari konfigurasi yang akan dibangun serta metode-metode yang akan diterapkan pada topik masalah yang diambil.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab ini menyajikan penerapan metode-metode yang digunakan dalam membangun keamanan sistem jaringan. Serta pengujian simulasi keamanan tersebut.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang sudah diperoleh dari hasil penulisan tugas akhir ini