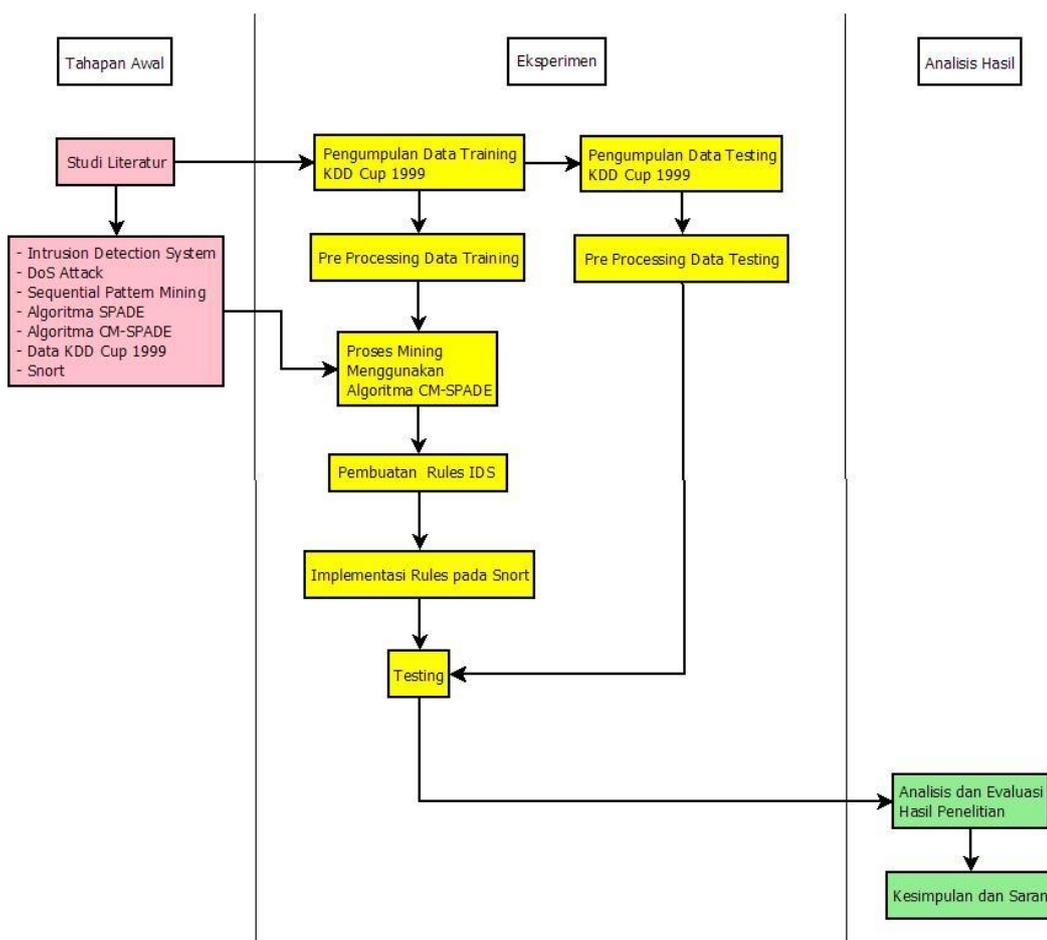


## BAB III METODOLOGI PENELITIAN

Pada bab ini akan dijelaskan mengenai metodologi penelitian yang dilakukan selama penelitian meliputi desain penelitian, alat dan bahan penelitian.

### 3.1. Desain Penelitian

Urutan langkah-langkah apa saja yang penulis kerjakan untuk menyelesaikan penelitian ini tertuang dalam desain penelitian. Dalam desain penelitian tersebut tergambar alur proses dari awal sampai ditemukan hasil akhir yang sesuai. Desain penelitian yang digunakan dalam penelitian ini dapat dilihat pada gambar 3.1.



Gambar 3.1 Desain Penelitian

### 3.1.1. Studi Literatur

Studi literatur dilakukan dengan cara mengadakan sebuah survei dan pembahasan literatur pada bidang IDS. Studi merupakan gambaran singkat dari pembelajaran IDS, baik pengertian, metode-metode yang bisa digunakan, serta hasil-hasil penelitian sebelumnya. Dalam studi literatur penelitian ini, survei dan pembahasan lebih difokuskan kepada materi IDS dan juga teknik *data mining*.

### 3.1.2. Pengumpulan Data Training KDD Cup 1999

Pada tahapan ini, penelitian akan berfokus kepada pengumpulan data-data yang akan dijadikan data *training* pada proses pembentukan IDS. Data set yang digunakan sebagai data *training* adalah data pada KDD Cup tahun 1999, yang dimana data tersebut terdiri dari atribut-atribut data akses pada suatu jaringan.

### 3.1.3. Pengumpulan Data Testing KDD Cup 1999

Pada tahapan ini tidak akan terlalu jauh berbeda dari tahapan 3.1.2, yang membedakan hanyalah data yang akan diambil pada proses ini adalah data yang akan dijadikan data *testing* untuk menguji IDS yang nantinya akan dibangun.

### 3.1.4. Preprocessing Data Set

*Preprocessing* adalah salah satu tahapan yang dilakukan dalam pendekatan *data mining*. *Preprocessing* dilakukan karena beberapa alasan, diantaranya adalah karena (1) terdapat data yang *incomplete*, dalam artian memiliki atribut yang kurang jika dibandingkan dengan data lainnya, (2) terdapat data-data yang dapat merusak normalitas dari data karena memiliki nilai *outlier* yang berbeda jauh dari data normal, atau dengan kata lain data tersebut memiliki *noise*, dan (3) terdapat ketidakcocokkan dalam penggunaan atribut dalam data, atau terjadinya *inconsistent*.

*Preprocessing* dilakukan untuk mendapatkan kualitas data yang terbaik, yaitu data yang akurat, lengkap, konsisten, normal dan representative.

### 3.1.5. Proses Mining Menggunakan Algoritma CM-SPADE

Pada tahapan ini, data yang sebelumnya telah melalui proses *preprocessing* pada tahap 3.1.4, dalam artian data telah memiliki kualitas bagus, selanjutnya akan memasuki tahap *data mining*.

Pada tahapan ini, data akan dicari pola penyebarannya berdasarkan kelas target yang telah ditentukan, yaitu tipe akses data pada jaringan.

### **3.1.6. Pembuatan *Rules* dan Model IDS**

Pada tahapan ini, data yang telah ditemukan pola penyebarannya pada tahap 3.1.5, selanjutnya akan dianalisis untuk ditentukan, mana yang merupakan data normal, dan mana yang merupakan data abnormal. Data normal menunjukkan bahwa data tersebut merupakan akses legal, sedangkan data abnormal menunjukkan bahwa data tersebut merupakan akses ilegal dan berupa intrusi kedalam sistem. Selanjutnya akan dibangun sebuah model yang bersifat *anomaly-based* untuk selanjutnya dimasukkan sebagai *rules* IDS.

### **3.1.7. Implementasi Rules pada Snort**

Tahapan ini adalah implementasi model IDS. Pada tahapan ini, pola-pola yang telah ditemukan pada tahapan-tahapan sebelumnya, yaitu mulai dari tahapan 3.1.5 sampai 3.1.6, akan diimplementasikan kedalam perangkat lunak sebagai *rules* dalam mendeteksi intrusi pada IDS.

### **3.1.8. Testing**

Pada tahapan ini akan dilakukan *testing* terhadap IDS yang telah dimodifikasi dan ditambahkan *rules* berdasarkan hasil *data mining*. *Testing* dilakukan dengan cara membuat sebuah simulasi akses jaringan terhadap suatu server, baik akses yang tergolong normal, maupun akses yang tergolong serangan. Setelah simulasi selesai, hasil performa IDS dapat dilihat melalui log yang dihasilkan oleh SNORT.

### **3.1.9. Analisis dan Evaluasi Hasil Penelitian**

Tahapan ini akan menganalisa data hasil pengujian, dan selanjutnya akan dilakukan komparasi dengan data pengujian penelitian sebelumnya.

Proses analisis dan evaluasi meliputi berbagai macam aspek hasil uji coba, yaitu tingkat akurasi IDS yang dibangun, waktu kerja proses yang dibutuhkan, nilai *false positive*, nilai *false negative*, serta alasan-alasan dibalik hasil-hasil tersebut.

### 3.1.10. Kesimpulan dan Saran

Tahapan ini merupakan akhir dari serangkaian proses penelitian. Pada tahapan ini akan dibahas dan ditarik kesimpulan dari tahapan 3.1.10, serta akan diberikan saran berupa layak tidaknya penggunaan metode yang diajukan dan saran akan penelitian-penelitian selanjutnya.

## 3.2. Alat dan Bahan

Pada sub-bab ini akan dipaparkan alat dan bahan penelitian yang digunakan dalam penelitian ini. Alat penelitian meliputi perangkat yang di butuhkan baik perangkat keras maupun perangkat lunak untuk pengembangan program. Bahan penelitian meliputi data baik *testing* maupun *training*, literatur pendukung dan penelitian yang berelasi yang mendukung penelitian.

### 3.2.1. Alat Penelitian

Alat penelitian yang digunakan adalah seperangkat komputer yang dilengkapi sistem operasi dan perangkat lunak pendukung dengan spesifikasi sebagai berikut:

a. Perangkat Keras:

- *Processor AMD® A10-5750M APU*
- *Random Access Memory (RAM) 8 GB DDR3*
- *Video Graphic Array Card Radeon HD 8670M 2 GB*
- *Solid State Drive (SSD) 120 GB*
- *Hard Disk Internal 1 TB*
- *Monitor 15,6' LED*
- *Mouse dan Keyboard*

b. Perangkat Lunak:

- *Sistem Operasi Linux Mint 17.3 Cinnamons 64 bit*
- *Sistem Operasi Windows 10*
- *Notepad++*
- *SPMF v2.38*

- Weka v3.8

### **3.2.2. Bahan Penelitian**

Bahan penelitian yang digunakan adalah berkas seperti jurnal, buku, artikel, artikel di *web*, dan dokumentasi yang mendukung penelitian ini. Bahan penelitian di dapat dari observasi di perpustakaan, internet dan sumber lainnya. Selain itu data yang merupakan bahan penelitian didapat dari internet yang telah di validasi oleh ahli dan merupakan data yang telah digunakan oleh banyak penelitian yang berelasi dengan penelitian ini.