BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Garut adalah sebuah instansi yang bertanggung jawab atas pengolahan informasi dalam lingkungan Pemerintahan Kabupaten Garut. Yang mana dalam dekade terakhir keamanan jaringan server telah menjadi salah satu bagian yang sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya dilingkungan Diskominfo Kabupaten Garut. Sebuah jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindahan oleh pihak yang tidak bertanggung jawab.

Berdasarkan hasil wawancara dengan bapak Rio Travolta selaku kepala Divisi IT Diskominfo Kabupaten Garut menyatakan, bahwa masalah yang kerap terjadi dalam keamanan jaringan di IT Diskominfo Kabupaten Garut ialah *spoofing*. Yaitu penyusup yang dapat terlihat seperti host yang dapat dipercaya serta secara diam-diam dan leluasa mencuri identitas dan kata sandi data client pada server pegawai secara ilegal yang mengakibatkan data pegawai bocor ke tangan yang tidak bertanggung jawab.

Masalah lainnya yang juga kerap terjadi yaitu *Distributed Denial of Service (DDoS)* yang mana masalah ini adalah sebuah percobaan penyerangan dari beberapa sistem komputer penyerang yang[menargetkan jaringan Diskominfo Kabupaten Garut agar jumlah *traffic* menjadi tinggi sampai server tidak bisa menghandle requestnya hal ini pernah terjadi diantara tanggal 1 November 2019 – 30 November 2019 dimana traffic yg awalnya diantara 3Mb byte/second melonjak tinggi menjadi 2 Gb byte/second dan membuat server down. Hal ini mengakibatkan terganggunya komunikasi antar komputer dijaringan Diskominfo Kabupaten Garut.

Untuk menghadapi masalah keamanan jaringan juga dapat menggunakan Suricata, Suricata merupakan perangkat lunak pendeteksi gangguan atau *Intrusion Detection and Prevention System (IDPS) open source* yang merupakan generasi lanjutan dari *IDS/IPS*. Suricata di bangun untuk alternatif *multi-threaded* untuk *Snort*. Sedangkan *Barnyard2* adalah *tool open source* sebagai penerjemah *alert*

unified dan log dari Suricata. *Barnyard2* dapat meningkatkan efisiensi Suricata dengan cara mengurangi beban pada sensor deteksi. *Barnyard2* bekerja dengan membaca *snort's unified logging output files* dan memasukkannya ke dalam database. Dan *Snorby* adalah salah satu aplikasi *web (front-end)* berbasis ruby on rails untuk memantau sistem keamanan jaringan komputer dengan tampilan antarmuka berbasis *GUI (Graphical User Interface)*.

Berbagai upaya untuk menyelesaikan masalah seperti yang telah dipaparkan diatas salah satunya dilakukan oleh Sofyan Hadi dan Periyadi, S.T., M.T. yang berjudul Implementasi Network Intrusion Detection System pada Sistem Smart Identification yang mana pada penelitian tersebut Dengan adanya Suricata sebagai IDS yang digunakan, setiap serangan yang ditujukan ke dalam jaringan akan dideteksi oleh Suricata dengan pengecekan terhadap rules yang digunakan. Setiap serangan yang sudah masuk ke dalam database akan ditampilkan melalui web interface Snorby[1]. Penelitian lainnya dilakukan oleh Dwi Kuswanto yang berjudul Unjuk Kerja Intrusion Prevention Sistem (IPS) Berbasis Suricata Pada Jaringan Lokal Area Network Laboratorium Tia+ Teknik Informatika, Universitas Trunojoyo yang mana pada penelitian tersebut bahwa Implementasi Suricata dan IPTables yang telah dikonfigurasi menjadi modus inline dapat bekerja dengan baik[2]. Penelitian lainnya dilakukan oleh Asep Fauzi Mutaqin yang berjudul Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort yang mana pada penelitan tersebut Barnyard2 dapat bekerja dengan membaca snort's unified logging output files dan memasukkannya ke dalam database. Jika database tidak tersedia maka Barnyard2 akan memasukkan semua data ketika database tersedia kembali sehingga tidak ada alert atau log yang hilang[3].

Berdasarkan dari masalah dan penelitian tersebut, maka penulis merancang sistem Intrusion Detection and Prevention System serta mengimplementasi Suricata, Barnyard2 dan Snorby agar dapat menangani suatu penyerangan berdasarkan alert yang telah ditampung pada database dan juga dapat memberikan gambar visual tentang serangan yang baru saja terjadi serta sebagai penunjang keamanan jaringan server.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya terdapat beberapa masalah mengenai kebutuhan yang diperlukan oleh Diskominfo Kabupaten Garut. Adapun masalah-masalah tersebut dapat diidentifikasi sebagai berikut.

1. Penyusup yang dapat terlihat seperti host yang dapat dipercaya serta secara diam-diam dan leluasa mencuri identitas dan kata sandi data client pada server pegawai secara ilegal.
2. Penyerang yang menargetkan jaringan Diskominfo Kabupaten Garut agar jumlah *traffic* menjadi tinggi sampai server tidak bisa menghandle requestnya.

1.3 Maksud dan Tujuan

Berdasarkan permasalahan yang diteliti, maka maksud dari penelitian ini adalah melakukan perancangan dan mengimplementasikan menggunakan Suricata, Barnyard2 dan Snorby. Adapun tujuan yang akan dicapai dalam penelitian ini adalah sebagai berikut.

1. Mengimplementasikan Suricata, Barnyard2 dan Snorby agar dapat digunakan untuk mendeteksi serangan penyusup yang ditujukan pada jaringan Diskominfo Kabupaten Garut.
2. Membangun sebuah sistem yang mampu memberikan informasi mengenai aktivitas serangan jaringan kepada *administrator* jaringan, sehingga dapat dipelajari pola serangan yang terjadi terhadap jaringan serta menunjang keamanan jaringan agar lebih baik dan aman.

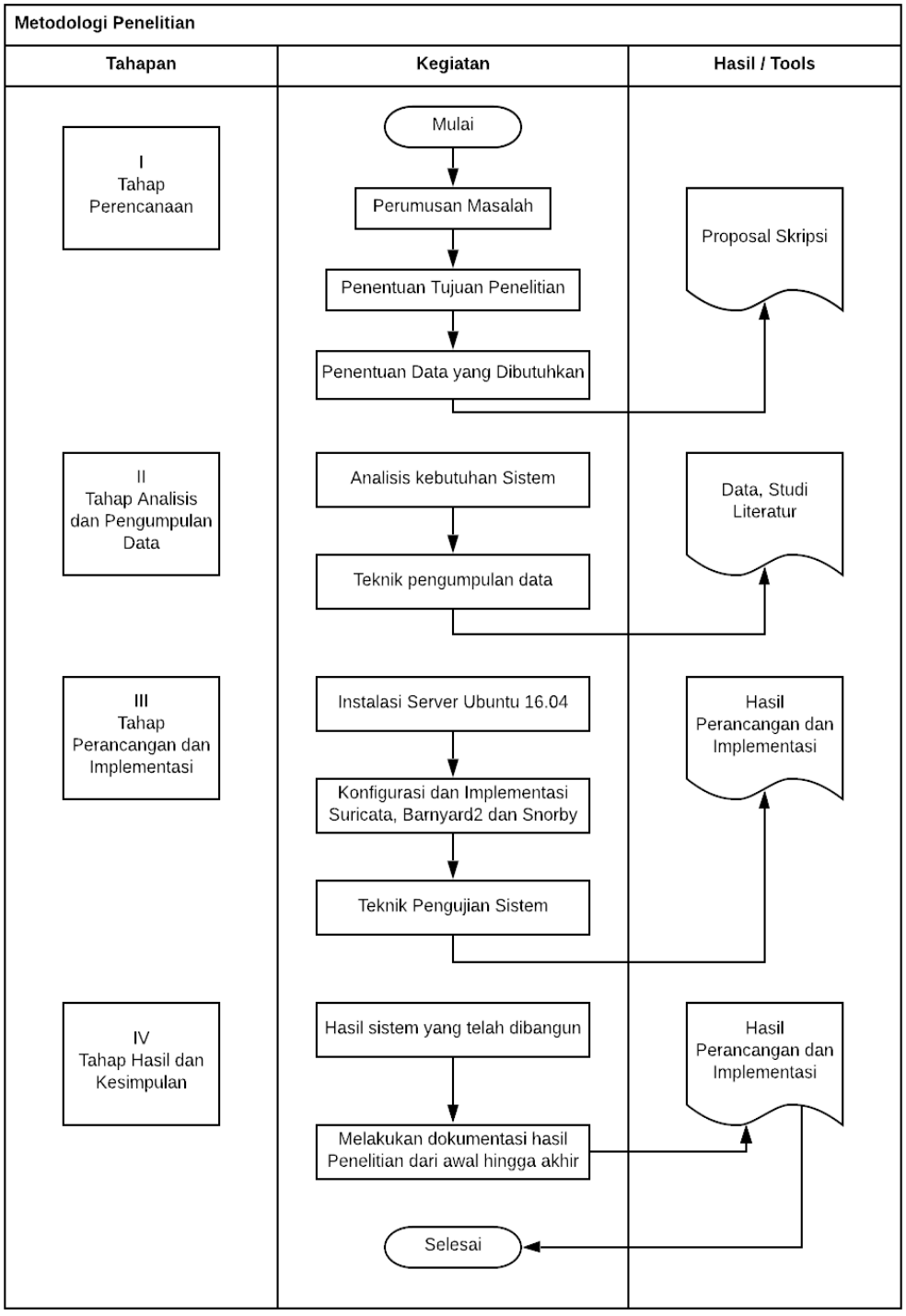
1.4 Batasan Masalah

Penelitian ini dibuat dengan beberapa batasan masalah agar lebih terfokus sesuai dengan tujuan yang akan dicapai. Pembatasan masalah dilakukan agar penulisan skripsi dapat memberikan pemahaman yang terarah sesuai dengan yang diharapkan. Batasan masalah dalam pembangunan sistem ini adalah sebagai berikut.

1. Pengimplementasian Suricata, Barynard2 dan Snorby menggunakan Ubuntu Versi 16.04
2. Data masukan yang digunakan ialah penetrasi testing simulasi yang akan dilakukan dalam tahap pengujian.
3. Pada prosesnya, Suricata akan mendeteksi dan Barnyard2 akan menampung log hasil deteksi tersebut dan Snorby menampilkan hasil deteksi tersebut
4. Menggunakan *IP-Address* versi 4 dalam pengimplementasianya.
5. Serangan pada jaringan akan dilakukan dalam pengujian berbentuk simulasi.
6. Serangan yang akan digunakan dalam pengujian ditentukan dan terbatas.
7. Keluaran dari sistem menghasilkan pemberitahuan aktifitas serangan yang telah terjadi berupa informasi dari penyerang dan alert atas serangan yang yang telah dilakukan.

1.5 Metodologi Penelitian

Metodologi yang digunakan pada penelitian ini adalah metodologi kuantitatif, yang berarti penelitian dilakukan secara sistematis. Penelitian dilakukan dengan urutan dan prosedur tertentu yang bersifat tetap. Pendekatan kuantitatif merupakan sebuah metodologi penelitian yang didasari oleh filsafat positivisme logikal, berdasarkan aturan – aturan yang ketat mengenai logika, kebenaran, hukum – hukum dan prediksi. Berikut metode penelitian dapat dilihat pada **Gambar 1.1**



Gambar 1.1 Metodologi Penelitian

Adapun penjelasan dalam tahap penelitian pada **Gambar 1.1** adalah sebagai berikut.

A. Tahap Perencanaan

Tahap perencanaan merupakan tahap awal dalam penelitian, kegiatan yang dilakukan adalah sebagai berikut:

1. Perumusan Masalah

Perumusan masalah adalah proses yang diperlukan untuk mengetahui inti dari persoalan, penyebab permasalahan yang sering terjadi di keamanan server.

2. Penentuan Tujuan Penelitian

Untuk mendukung pencapaian sasaran penelitian, tahapan selanjutnya adalah penentuan tujuan dari penelitian yang dilakukan. Tujuan penelitian yang dilakukan adalah sebagai berikut:

a. Membangun sebuah sistem yang mampu memberikan informasi/laporan aktivitas serangan jaringan kepada *administrator*, sehingga dapat dipelajari pola serangan yang terjadi terhadap jaringan serta menunjang keamanan jaringan agar lebih baik dan aman.
b. Mengimplementasikan Suricata, Barnyard2 dan Snorby agar dapat digunakan untuk mengamankan jaringan Diskominfo Kabupaten Garut dari serangan-serangan jaringan.

3. Penentuan Data yang Dibutuhkan

Untuk mempermudah penulis dalam melakukan analisis, maka perlu ditentukan beberapa data seperti:

a. Teori-teori yang berhubungan dengan perancangan dan implementasi Suricata, Barynard2, Snorby dan *IDPS* sebagai keamanan server jaringan kompter.
b. Teknik analisa yang digunakan.
c. Menentukan kebutuhan data primer dan data sekunder.

B. Tahap Analisis dan Pengumpulan Data

Tahap ini merupakan tahap yang dilakukan setelah tahap perencanaan. Setelah data ditentukan, maka selanjutnya adalah mengumpulkan data tersebut. Tahapan ini berisi tentang proses dalam pengumpulan data, baik data primer maupun data skunder. Tahapannya adalah sebagai berikut:

1. Analisis Kebutuhan Sistem

Analisis kebutuhan sistem yang akan dibangun dimulai dari analisis studi kasus hingga analisis terhadap data yang telah dibutuhkan dalam membangun sistem. Berikut beberapa alasan kenapa pada penlitian ini menggunakan Suricata, Barnyard2 dan Snorby.

a. Suricata.

Suricata adalah IDS, IPS dan monitoring engine untuk jaringan yang berkinerja tinggi. Suricata adalah open source dan dimiliki oleh masyarakat yang dikelola yayasan non-profit, Open Information Security Foundation (OISF). Keunggulan suricata adalah *Highly Scalable* yang mana suricata adalah multi threaded. Ini berarti dapat menjalankan satu instance dan akan menyeimbangkan beban pengolahan di setiap prosesor pada sensor Suricata yang dikonfigurasi untuk menggunakan. Hal ini memungkinkan perangkat keras komoditas untuk mencapai kecepatan 10 gigabit pada lalu lintas real tanpa mengorbankan cakupan ruleset. Hal lainnya ialah peneliti dapat menulis rules untuk setiap aturan protokol.

b. Barnyard2

Barnyard2 adalah interpreter open source untuk file keluaran biner Sucirata unified2. Penggunaan utamanya memungkinkan Suricata untuk menulis ke database dengan cara yang efisien dan membiarkan tugas mengurai data biner ke dalam berbagai format menjadi terpisah proses yang tidak akan menyebabkan Suricata kehilangan lalu lintas jaringan. Alasan pada penelitian ini menggunakan barnyard2 adalah barnyard2 dapat menerjemahkan unified suricata untuk dimasukan kedalam database MySQL.

c. Snorby

Snorby adalah aplikasi web ruby on rails untuk pemantauan keamanan jaringan yang berinteraksi dengan sistem deteksi intrusi populer saat ini (Suricata). Konsep dasar di balik Snorby adalah kesederhanaan, pengorganisasian, dan kekuatan. Tujuan proyek ini adalah untuk membuat aplikasi gratis, open source, dan sangat kompetitif untuk pemantauan jaringan baik untuk penggunaan pribadi maupun perusahaan. Adapaun alasan penggunaan snorby pada penelitian ini ialah antarmuka interface yang sangat friendly dalam hal penggunaannya. Dan snorby dapat menampilkan rentang waktu penyerangan dan detail dari serangan yang telah dilakukan oleh penyerang.

2. Teknik Pengumpulan Data

Berikut ini adalah teknik pengumpulan data pada penelitian yang dilakukan.

a. Studi Pustaka

Studi pustaka yaitu metode pengumpulan data berupa literatur, jurnal, paper, dan dokumen lainnya yang berkaitan dengan kajian mengenai judul penelitian.

b. Data

Teknik pengumpulan data dengan mencari packet apa saja yang diperlukan dalam mengiplementasikan dan juga Suricata, Barnyard2, dan Snorby.

C. Tahap Perancangan dan Implementasi

Tahap ini merupakan tahap yang dilakukan setelah tahap analisis dan pengumpulan data. Tahapan ini berisi tentang proses instalasi, perancangan dan implementasi serta teknik pengujian yang digunakan dalam penelitian ini. Adapun tahapannya adalah sebagai berikut:

1. Instalasi Server Ubuntu 16.04

Pada tahap ini dilakukan menginstall Server Ubuntu 16.04 dan mengkonfigurasinya menjadi sebuah server untuk kebutuhan penelitian ini. Instalasi ini meliputi penginstalan paket-paket yang berhubungan dengan Suricata, Barynard2 dan Snorby.

2. Perancangan dan Implementasi Suricata, Barynard2, Snorby

Pada tahap ini dilakukan perancangan dan implementasi atas analisis dan pengumpulan data yang telah dilakukan, serta mengkonfigurasi tools – tools untuk merancang sistem yang akan dibangun.

3. Teknik Pengujian Sistem

Pada tahap ini dilakukan pengujian terhadap sistem yang sudah dibangun dengan beberapa teknik pengujian yaitu :

a. ***Spoofing*** yaitu Teknik serangan yang dilakukan attacker dengan cara memalsukan data sehingga attacker dapat terlihat seperti host yang dapat dipercaya.
b. ***DDOS (Distributed Denial Of Service)*** yaitu merupakan jenis serangan terhadap server pada suatu jaringan dengan metode menghabiskan resource yang dimiliki server sampai server tersebut tidak dapat menjalankan fungsinya untuk memberikan akses layananya.

D. Tahap Hasil dan Kesimpulan

Tahap ini merupakan tahap yang dilakukan setelah tahap perancangan dan implementasi. Adapun tahapannya adalah sebagai berikut:

1. Hasil Sistem yang Telah Dibangun

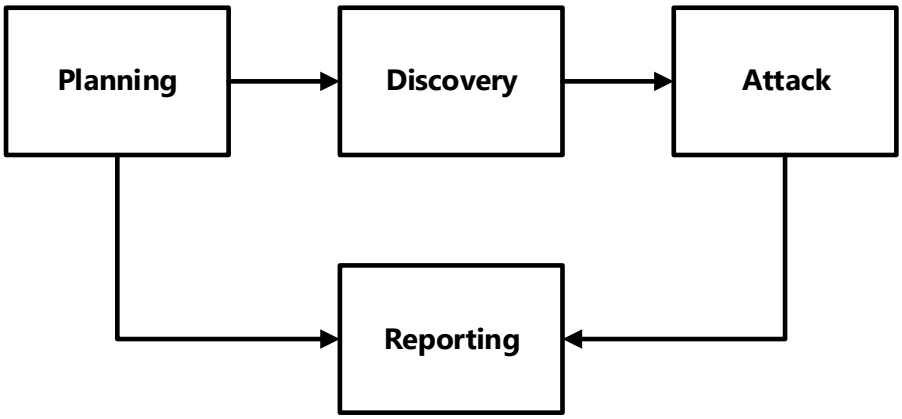
Pada tahap ini ialah menyimpulkan sistem yang telah dibangun dengan metodologi yang digunakan.

2. Dokumentasi Hasil Penelitian

Pada tahap ini ialah melakukan dokumentasi penulisan Draft Skripsi dari awal sampai akhir pengerjaan

1.6 Metode Penetrasi Jaringan

Metode penetrasi yang digunakan pada penelitian ini adalah NIST SP 800-115 *(National Institute for Science & Technology)*. NIST SP 800-115 merupakan metode yang mencangkup beberapa segala uji penetrasi. Metode ini memiliki empat tahap pengujian yaitu. Planning, Discovery, Attack, and Reporting. Gambar metode *National Institute for Science & Technology* dapat dilihat pada **Gambar 1.2**.



Gambar 1.2 Metode NIST SP 800-115

Berikut adalah tahapan-tahapan yang dilakukan dalam penelitian ini

A. Planning

Planning adalah tahap dimana seorang *pentester* berusaha mengumpulkan sebanyak mungkin informasi mengenai perusahaan target yang bisa didapatkan dengan berbagai metode dan berbagai media. Hal yang perlu dijadikan dasar dalam pengumpulan informasi adalah *Covert Gathering, Footprinting,* Identifikasi mekanisme perlindungan.

B. Discovery

Discovery merupakan pendefinisian dari pendekatan penemuan ancaman. *Discovery* diperlukan untuk pelaksanaan pengujian penetrasi yang benar. Pendekatan permodelan yang di maksud adalah pengamatan terhadap

target yang bertujuan untuk mengetahui proses bisnis target agar lebih mudah dalam menentukan serangan. Hal yang perlu dijadikan dasar *Discovery* adalah analisis tujuan bisnis.

C. Attack

Attack adalah tahap dimana seorangan *pentester* melakukan serangan pada target. Walaupun demikian tahap ini kebanyakan dilakukan dengan metode *brute force* tanpa memiliki unsut presisi. Seseorang *pentester* hanya akan melakukan *attack* ketika dia sudah mengetahui secara pasti apakah serangan yang dilakukan berhasil atau tidak, namun tentu saja ada kemungkinan tidak terduga dalam sistem keamanan target. Walaupun begitu, sebelum melakukan serangan, *pentester* harus tahu kalau target mempunyai celah keamanan yang bisa di gunakan. Melakukan serangan secara membabi-buta dan berharap sukses bukanlah metode yang produktif. Seorangan *pentester* selalu menyempurnakan analisisnya terlebih dahulu sebelum melakukan serangan yang efektif

D. Reporting

Reporting adalah bagian paling penting dalam kegiatan *pentest.* Seorang *pentester* menggunakan *report (*laporan*)* untuk menjelaskan pada perusahaan mengenai *pentesting* yang dilakukan seperti: apa yang di lakukan, bagaimana cara melakukannya, resiko yang bisa terjadi dan yang paling utama adalah cara untuk memperbaiki sistemnya.

1.7 Sistematika Penulisan

Sistematika penulisan ini disusun untuk memberikan gambaran umum tentang penulisan tugas akhir yang akan dilakukan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB 1 PENDAHULUAN

Pada bab ini membahas mengenai latar belakang masalah yang ditemukan, identfikasi masalah, maksud dan tujuan, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Pada bab ini membahas mengenai tujuan umum Penelitian pada Diskominfo Kabupaten Garut dan pembahasan berbagai konsep dasar mengenai Jaringan Komputer serta membahas tentang keamanan jaringan komputer meliputi serangan-serangan dan teknik-teknik dalam penyerangan jaringan komputer.

BAB 3 ANALISIS DAN PERANCANGAN

Bab ini berisi pemaparan analisis masalah, analisis kebutuhan data, analisis basis data, analisis kebutuhan non fungsional, dan analisis kebutuhan fungsional. Hasil dari analisis kemudian diterapkan pada perancangan perangkat lunak yang terdiri dari perancangan sistem, testing sistem, perancangan antarmuka dan jaringan semantik.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini membahas implementasi dalam bahasa jaringan yaitu implementasi kebutuhan perangkat keras dan perangkat lunak, implementasi basis data, implementasi antarmuka dan tahap – tahap dalam melakukan pengujian perangkat lunak.

BAB 5 KESIMPULAN DAN SARAN

Bab ini membahas tentang kesimpulan yang sudah diperoleh dari hasil penulisan tugas akhir dan saran mengenai pengembangan aplikasi untuk masa yang akan datang.