BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi saat ini berkembang dengan sangat pesat. Perkembangan tersebut juga mempengaruhi penggunaan teknologi dalam kehidupan sehari-hari, termasuk teknologi informasi. Teknologi informasi adalah sarana dan prasarana (*hardware*, *software*, *useware*) sistem dan metode untuk memperoleh, mengirimkan, mengolah, menafsirkan, menyimpan, mengorganisasikan, dan menggunakan data secara bermakna (Warsita, 2008). Selain teknologi, manusia juga dituntut untuk berkembang sehingga dapat mengimbangi pekembangan teknologi yang ada.

Perkembangan teknologi yang dimanfaatkan dengan baik dapat menjadi hal yang positif bagi mereka yang bertanggung jawab dalam menggunakan untuk berbagai hal. Namun disisi yang lain, perkembangan teknologi informasi juga menimbulkan dampak yang buruk seperti kejahatan komputer (*computer crime*) (Rahardjo, 2005). Hal tersebut membawa kekhawatiran bagi para pengguna teknologi informasi, sehingga keamanan dari teknologi informasi menjadi hal yang sangat penting untuk diperhatikan.

Website merupakan salah satu pemanfaatan komputer yang terintegrasi dengan internet. *Website* dapat diartikan sebagai kumpulan halaman-halaman web beserta file-file pendukungnya, seperti file gambar, video, dan file digital yang disimpan pada sebuah web server yang umumnya dapat diakses melalui internet.

Website juga dapat diartikan sebagai sekumpulan folder dan file yang mendukung banyak perintah dan fungsi-fungsi tertentu, seperti fungsi tampilan, fungsi menangani penyimpanan data, dan fungsi lainnya (Hartono, 2008).

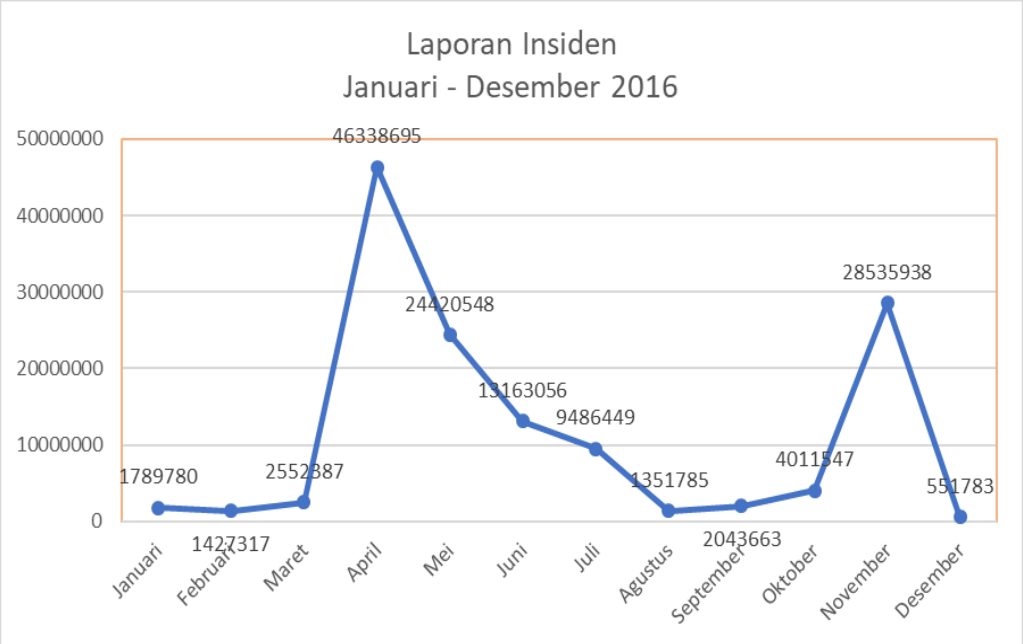
Pratama (2013) mengemukakan bahwa *website* disediakan melalui jalur internet sehingga dapat diakses seluruh dunia selama terkoneksi dalam jaringan internet tanpa terbatas ruang dan waktu. Banyak ancaman keamanan terjadi dalam bentuk pencurian virtual di internet. Seorang pencuri internet dapat mengakses

sistem informasi dan mencuri informasi penting seperti *password* dan informasi pribadi dalam hitungan detik.

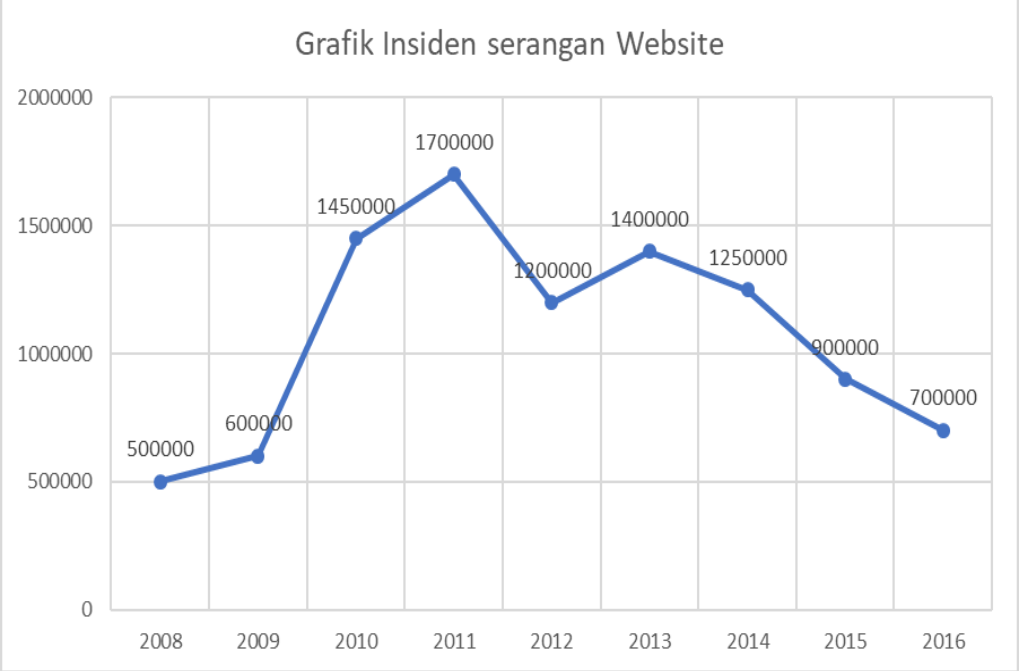
Keamanan sistem informasi sangat dibutuhkan sebagai bentuk pengamanan terhadap data dan informasi yang dimiliki oleh sebuah instansi. Hal tersebut penting karena jika data dan informasi pada sebuah instansi dapat diakses oleh orang yang tidak bertanggung jawab, maka keamanan data dan informasi tersebut dapat disalah gunakan. Sistem keamanan informasi memiliki empat tujuan (Paryati, 2008) antara lain: Kerahasiaan (*Confidentiality*), Ketersediaan (*Availability*), Integritas (*Integrity*) dan Penggunaan yang sah (*Legitimate Use*).

Kerahasian (*Confidentiality*) berarti melindungi informasi dari akses yang tidak diizinkan, Ketersediaan (*Availability*) berarti melindungi informasi agar tetap dapat diakses, Integritas (*Integrity*) berarti melindungi dari perubahan data yang tidak diizinkan, dan Penggunaan yang sah (*Legitimate Use*) berarti melindungi akses data dari orang yang tidak berhak. Keempat komponen tersebut berkaitan erat dengan sistem perlindungan terhadap informasi.

Ancaman terhadap keamanan informasi tidak dapat dihindari. Ancaman-ancaman ini dapat berubah menjadi serangan dan insiden terhadap teknologi informasi yang dapat menggagu sistem dari keamanan informasi. Pada tahun 2016 telah terjadi berbagai insiden serangan. Insiden serangan yang terjadi pada *website* sebanyak 46,338,695 dibulan April tahun 2016. Berikut adalah data insiden serangan yang terjadi pada tahun 2016 di Indonesia:

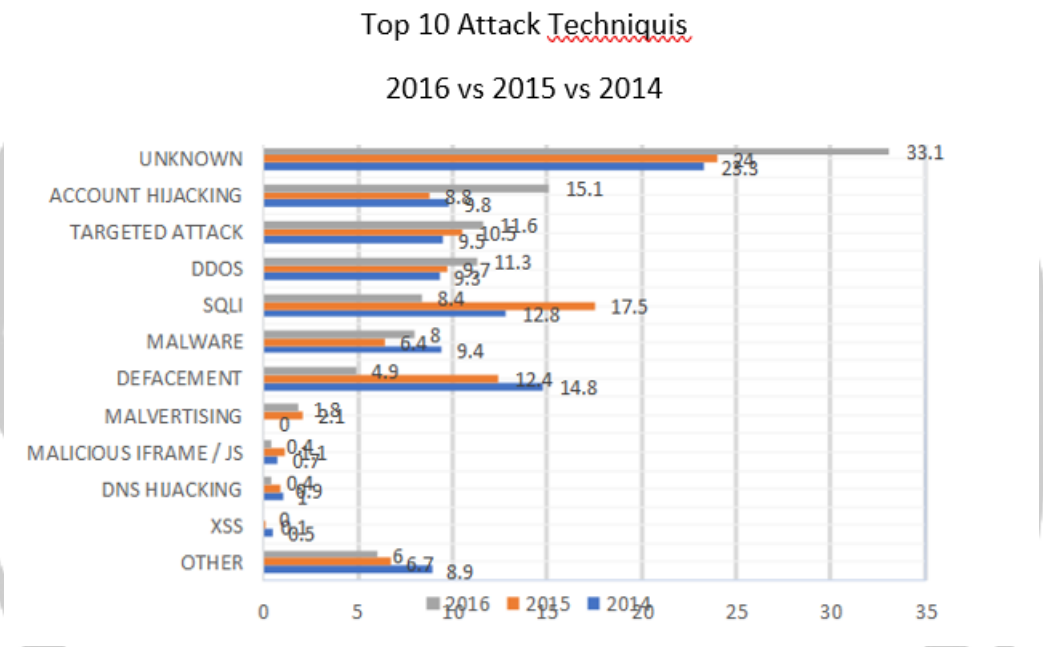


Gambar 1.1: *Traffic* laporan insiden serangan tahun 2016 di Indonesia (Sumantri, 2017).



Gambar 1.2 Grafik insiden serangan *website* (Sumantri, 2017).

Sumantri (2017) lebih spesifik mengemukakan data terkait insiden serangan yang terjadi pada *website* di Indonesia. Melalui grafik diatas dapat dilihat bahwa insiden serangan pada website paling banyak terjadi di tahun 2011. Insiden serangan pada *website* yang terjadi di Indonesi dilakukan dengan berbagai teknik Sumantri (2017). Berikut sepuluh global teknik serangan yang terjadi mulai tahun 2014 hingga 2016:



Gambar 1.3. sepuluh global teknik serangan yang terjadi pada tahun 2014, 2015, dan 2016 (Sumantri, 2017).

Gambar 1.1, 1.2, dan 1.3 menunjukan banyaknya jenis serangan yang terjadi pada *website*. Serangan-serangan tersebut merupakan hasil pengaduan insiden serangan yang diterima oleh ID-SIRTII. ID-SIRTII (*Indonesia Security Incident Response Team on Internet Infrastructure*) merupakan tim yang dibentuk oleh Pemerintahan Indonesia yang bertugas untuk menangani insiden seperti pemantauan, pendeteksian terhadap ancaman insiden serangan. Selain respon dalam menangani insiden, penting juga untuk dilakukan upaya-upaya yang dapat mencegah terjadinya insiden. Setidaknya kemungkinan terjadinya insiden dapat diperkecil, walaupun tidak semua insiden dapat dicegah.

Berdasarkan latar belakang tersebut, penelitian ini akan membahas mengenai proses penanganan dan pencegahan yang dilakukan dalam menangani sebuah insiden serangan pada *website*. Proses penanganan dan pencegahan tersebut dimulai dari tahap persiapan (*preparation*); tahap deteksi dan analisis (*dectection & analysis*); tahap penanganan, pembersihan, dan pemulihan (*containment, eradiction & recovery*); dan tahap pasca insiden (*lesson learned*).

Insiden serangan dapat ditangani menggunakan berbagai metode. Metode penanganan insiden serangan yang pernah dijadikan panduan dalam melakukan penelitian antara lain: COBIT 5, ISO/IEC 27001, ITIL V3, dan NIST 800-61.

Penelitian yang dilakukan oleh (Ciptaningrum, et al., 2015) membahas mengenai standar operasional dan prosedur manajemen pengamanan sistem informasi dan telekomunikasi di lingkungan Pemerintah Kota Yogyakarta. Metode yang digunakan dalam penelitian tersebut adalah COBIT 5, dan hasil dari penelitian tersebut adalah pelaksanaan audit keamanan sistem informasi pada Kantor Pemerintahan Kota Yogyakarta.

Penelitian yang dilakukan oleh Chazar (2015) menggunakan metode ISO/IEC 27001 sebagai standar yang digunakan untuk mengetahui kebutuhan penerapan sistem informasi. Hasil dari penelitian ini adalah penerapan dan pengelolaan keamanan sistem informasi pada sebuah instansi.

Rachmi et al., (2014) melakukan penelitian mengenai permasalahan TI (Teknologi Informasi) dan upaya dalam meningkatkan layanan dengan menggunakan metode ITIL V3. Hasil dari penelitian tersebut adalah pembuatan SOP (*Standard Operating Procedur*) *service desk*.

Penelitian lain yang dilakukan oleh Andy (2016) membahas mengenai cara penanggulangan insiden DDos pada jaringan. Dalam penelitian tersebut dijelaskan bahwa penanganan insiden DDos memang tidak mudah, namun dapat dilakukan meskipun terkadang memakan banyak waktu dan sumber daya dalam prosesnya. Dengan penanganan yang baik dan benar sesuai dengan rekomendasi dari NIST 800-61 diharapkan agar insiden DDos dapat ditangani dengan lebih efektif dan efisien.

Beberapa penelitian di atas menjadi pedoman peneliti dalam melakukan penelitian mengenai penanganan insiden serangan yang terjadi pada *website*. Penanganan dalam penelitian ini akan mengikuti rekomendasi yang diberikan oleh NIST 800-61. NIST 800-61 adalah dokumen standar yang dikembangkan oleh *National Institute of Standards and Teknologi* (NIST) yang mana merupakan dokumen yang berfokus membahas tentang penanganan insiden (*incident handling*) dan bersifat umum yang mana metode ini bisa digunakan oleh siapa pun terkait dengan *Cybersecurity*.

Berbeda dengan penelitian Andy (2016) yang membahas mengenai insiden pada DDos, penelitian ini lebih membahas mengenai insiden serangan yang terjadi pada *website* antara lain: *Sql Injection, Web Deface, dan DDoS*. Selain itu juga akan dibuat Standar Operasional Prosedur (SOP) untuk menangani insiden yang terjadi dalam sebuah instansi agar insiden dapat dicegah dan diminimalisir.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang masalah tersebut, maka peneliti mengajukan rumusan masalah sebagai berikut:

Bagaimana membuat Standar Operasional Prosedur (SOP) penanganan dan pencegahan insiden serangan pada *website* dengan menggunakan metode NIST 800-61 ?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Pembuatan Standar Operasional Prosedur (SOP) menggunakan metode NIST 800-61 hanya membahas tentang penanganan dan pencegahan insiden serangan pada website saja, tidak membahas penanganan dan pencegahan insiden serangan yang bukan website.
2. Kerangka kerja yang digunakan sebagai standar acuan penanganan insiden serangan adalah NIST.

1.4 Tujuan Penelitian

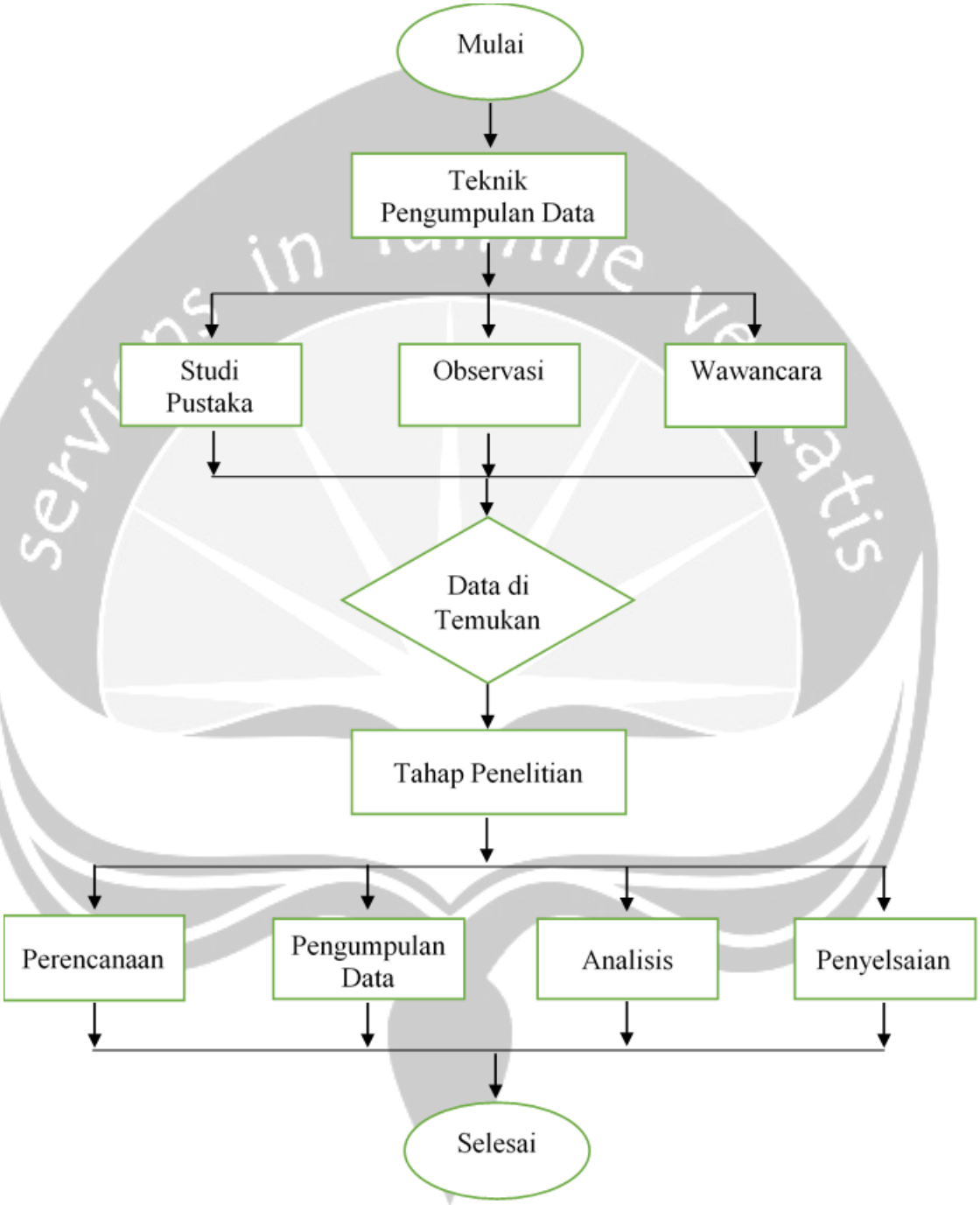
Tujuan yang ingin dicapai dari penelitian ini antara lain:

Membuat Standar Operasional Prosedur (SOP) penanganan dan pencegahan insiden serangan pada *website* dengan menggunakan metode NIST 800-61.

1.5 Metode Penelitian

Penelitian ini adalah penelitian yang menggunakan metode studi kasus, dimana penelitian dilakukan terhadap permasalahan data yang ada di lapangan. Peneliti melakukan pengamatan secara langsung terhadap objek penelitian, melakukan studi pustaka, dan mengumpulkan data yang relevan untuk kemudian dilakukan analisa agar dapat membuat SOP (*Standard Operating Procedure*) untuk penanganan dan pencegahan insiden serangan siber pada *website*. Berikut proses skema proses penelitian yang dilakukan peneliti:

Gambar 1.4. Skema proses penelitian



1.5.1 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan peneliti dalam mengumpulkan data-data mengenai topik penelitian penanganan dan pencegahan insiden serangan pada *website* adalah:

1. **Studi Pustaka**

   Metode penelitian studi pustaka adalah metode yang mempelajari literatur, buku dan segala informasi yang berkaitan dengan insiden serangan pada *website*. Fungsi dari metode ini adalah untuk menambah pengetahuan mengenai teori yang nantinya akan digunakan pada proses pengumpulan data dan analisis.

2. **Observasi**

   Observasi menurut Garayiban (dalam Emzir, 2010) merupakan pengamatan yang harus dilakukan secara alami dimana pengamat harus larut dalam situasi realistis dan alami yang sedang terjadi dan merupakan perhatian yang terfokus pada kejadian, gejala, atau suatu hal. Observasi adalah metode pengumpulan data melalui pengamatan perilaku dalam situasi tertentu kemudian mencatat peristiwa yang diamati dengan sistematis dan memaknai peristiwa yang diamati. Dalam penelitian ini peneliti akan melakukan observasi terhadap proses penanganan dan pencegahan insiden serangan yang terjadi pada *website*.

3. **Wawancara**

   Wawancara menurut Usman dan Setiady (2008) adalah tanya jawab lisan secara langsung. Wawancara dibagi menjadi dua yaitu wawancara terstruktur dan wawancara tak terstruktur (Mulyana, 2003). Wawancara terstruktur sering disebut sebagai wawancara baku yang pertanyaannya sudah disediakan, sedangkan wawancara tidak terstruktur mirip dengan percakapan informal yang sifatnya luwes dan susunan kata setiap pertanyaan dapat diubah saat wawancara.

   Pedoman wawancara yang digunakan dalam penelitian ini adalah wawancara tidak terstruktur yang hanya memuat secara garis besar apa yang akan ditanyakan.

1.5.2Tahap-tahap Penelitian

Alur penelitian yang dilakukan dibagi menjadi empat tahap yaitu:

1) Tahap perencanaan

Pada tahap perencanaan dilakukan perumusan masalah dan studi pustaka teori pendukung dalam melakukan penelitian.

2) Tahap pengumpulan data

Pada tahap pengumpulan data dilakukan memalui observasi dan wawancara.

3) Tahap analisis

Pada tahap analisis dilakukan dengan menganalisis data mengenai insiden serangan yang terjadi pada *website*.

4) Tahap penyelesaian

Pada tahap penyelesaian dilakukan pembuatan Standar Operasional Prosedur (SOP) yang dijadikan sebagai panduan penanganan dalam menangani insiden serangan yang terjadi pada *website* dan sebagai panduan pencegahan agar insiden serangan tidak terjadi lagi.

1.6 Sistematika Penelitian

Sistematika penulisan laporan tugas akhir ini dapat dijabarkan sebagai berikut:

BAB I PENDAHULUAN

Pada bab I berisi penjelasan singkat dan konsep dasar dalam pembuatan skripsi.

BAB II TINJAUAN PUSTAKA

Pada bab II berisi pembahasan skripsi dari mahasiswa lain dan penelitian yang pernah dilakukan oleh orang lain.

BAB III LANDASAN TEORI

Pada bab III berisi tentang uraian dasar teori yang akan digunakan penulis dalam melakukan perancangan dan pembuatan Standar Operasional

Prosedur (SOP) yang dapat dipergunakan sebagai pembanding atau acuan di dalam pembahasan masalah.

BAB IV ANALISIS DAN PERANCANGAN

Pada bab IV berisi tantang perancangan Standar Operasional Prosedur (SOP) dalam penanganan dan pencegahan insiden serangan siber pada *website*.

BAB V HASIL DAN PEMBAHASAN

Pada bab V berisi hasil dan implementasi penilaian terhadap Standar Operasional Prosedur (SOP) yang telah dirancang.

BAB VI KESIMPULAN DAN SARAN

Pada bab VI berisi tentang kesimpulan dari penelitian dan saran yang diberikan oleh peneliti.