BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Teknologi jaringan komputer selalu berkembang, meskipun saat ini sudah banyak *thesis* yang membahas jarinngan komputer, namun selalu ada hal yang menarik untuk dikaji ulang, terutama pada bidang keamanan jaringan komputer. Jaringan komputer sendiri didefinisikan sebagai suatu himpunan *interkoneksi* sejumlah komputer *autonomous*. Dalam bahasa populer dapat dijelaskan bahwa jaringan komputer merupakan sebuah kumpulan beberapa komputer yang terhubung satu sama lain yang dihubungkan melalui media perantara. [1]

Suatu jaringan komputer memerlukan suatu sistem keamanan untuk melindungi data dalam jaringan tersebut. Keamanan jaringan atau *network security* merupakan segala aktifitas pengamanan suatu jaringan atau *network,* tujuan dari keamanan jaringan ini untuk menjaga *usability, reliability, integrity,* dan *safety* dari suatu serangan. Selain empat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non – repudiation*. [2]

Network security harus mampu mencegah dan menghentikan berbagai potensi serangan agar tidak memasuki dan menyebar pada sistem jaringan. Serangan atau *Intrusion* itu sendiri dapat diartikan sebagai *"the act of*

thrusting in, or of entering into a placeor state whiteout invitation. Right or welcome, this unauthorized acces, or intrusion, is an attempt to compromise, or otherwise, to other network device. [3]

Ada beberapa potensi serangan, antara lain : [4]

(1) *Interruption*, perangkat sistem menjadi rusak atau tidak tersedia, serangan ini ditujukan kepada ketersediaan (*availability*) dari sistem.

(2) *Intercaption,* pihak tidak berwenang berhasil mengakses aset atau informasi.

(3) *Modification,* pihak tidak berwenang mampu mengubah aset atau informasi.

(4) *Fabrication*, pihak tidak berwenang menyisipkan objek palsu kedalam sistem.

Potensi serangan di atas dapat memberikan ancaman bagi suatu perusahaan berupa akses yang tidak terotorisasi pada informasi data perusahaan karena adanya suatu serangan. Untuk mencegah bobolnya data suatu perusahaan maka perlu suatu solusi p*reventif* untuk melindungi data tersebut, salah satu yang dapat dimanfaatkan untuk keamanan sistem jaringan suatu perusahaan dapat menerapkan suatu sistem deteksi serangan atau *(intrusion detection system)* pada jaringan perusahaan tersebut. "*Intrusion Detection System* adalah *"Detecting unauthorized use of attack upon system or network. An IDS designed and used to detect such attack or unauthorized use of system, network, andrelated resourceand then in many cases to deflect or deter them if possible*".[5]

Perancangan suatu keamanan jaringan komputer tidak harus memakan biaya yang besar, salah satu solusi untuk merancang suatu keamanan jaringan komputer dengan menggunakan *IDS snort* dan *honeypot, snort* dan *honeypot* merupakan sistem berbasis *open source*. Pemanfaatan sistem *snort* dan *honeypot* akan bekerja sesuai dengan konfigurasi yang telah dirancang. Dengan mengimplementasikan *snort* dan *honeypot* dalam arsitektur *IDS* diharapkan mampu bekerja lebih maksimal dalam menangani suatu serangan.

1.2. Rumusan Masalah

Dalam menyusun penelitian skripsi ini, ditentukan pokok-pokok masalah yang dibahas dan diteliti, yaitu menyusun suatu *prototyping intrusion detection system* berbasis *open source software.* Pada penelitian ini menggunakan IDS *snort, low interaction honeypot* mengunakan *honeyd* dan perancangan *high interaction honeypot honeynet* yang disesuaikan dengan *resource*.

Menganalisa dan membandingkan hasil pengukuran performansi *prototyping intrusion detection system snort* dan *honeypot* yang disesuaikan dengan *resource*.

1.3. Batasan Masalah

Agar penulisan penelitian skripsi ini mengarah pada pembahasan yang diharapkan dan terfokus pada pokok permasalahan yang ditentukan, maka

diperlukan batasan masalah dalam penelitian ini. Batasan masalah pada penelitian ini ditentukan dalam beberapa hal, sebagai berikut :

1) Sistem diinstall di lingkungan *Ubuntu,*
2) *Thread* yang dicakup pada penelitian ini ditentukan berdasar studi pustaka,
3) *Engine signature – based* IDS yang digunakan adalah *snort,*
4) *Engine* yang digunakan untuk *honeypot* adalah *honeyd,*
5) Rules *snort* dan *honeypot* yang digunakan merupakan versi *open source,*
6) Pola penyerangan yang dilakukan hanya dalam jaringan local (*Local Area Network*).

1.4. Tujuan Penelitian

Berdasarkan latar belakang masalah yang telah dicantumkan maka tujuan dari penelitian ini adalah sebagai berikut :

(1) Mendesain keamanan jaringan yang disusun dari *snort* dan *honeypot*
(2) Mengetahui perbandingan performa IDS *snort* dan *honeypot,*
(3) Mengamati *respon time* sistem terhadap serangan.

1.5. Manfaat Penelitian

Dalam pelaksanaan penelitian *"Analisa Perbandingan Performansi IDS Snort, Low Interaction Honeypot* dan *High Interaction Honeypot*" ini diharapkan dapat bermanfaat bagi :

1) Peneliti

Memberi pengetahuan mengenai suatu konsep jaringan komputer dan keamananya, serta mampu menangani suatu ancaman serangan dan ganguan pada suatu jaringan komputer.

2) Pembaca

Sebagai referensi dan rekomedasi jika akan melakukan penelitian dibidang keamana jaringan komputer peningkatan mutu keamanan jaringan.

3) Perusahaan dan Administrator Jaringan

Diharapkan dapat memberi suatu acuan atau menambah pikiran bagi administrator dalam penerapan monitoring jaringan.

1.6. Sistematika Penulisan

Sistematika penulisan ini bertujuan untuk memudahkan pemahaman, pembahasan dan memberi gambaran yang jelas mengenai keseluruhan penulisan karya ilmiah ini, maka penulis menyiapkan suatu sistematika dalam penyusunan karya ilmiah ini. Adapun sistematika penulisan karya ilmiah ini terdiri dari 5 bab, masing – masing bab tersebut berhubungan satu dan lainnya, adapun sistematika skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Bab ini berisikan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Bab ini akan membahas tentang telaah penelitian dan landasan teori dari karya ilmiah ini

BAB III : METODOLOGI PENELITIAN

Bab ini membahas tentang metode – metode yang digunakan dalam pengumpulan data penelitian.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini membahas tentang hasil dan pembahasan tentang *intrusion detection system snort, honeyd honeypot,* perancangan *honeynet honeypot* dan cara mengatasi serangan yang ada.

BAB V : PENUTUP

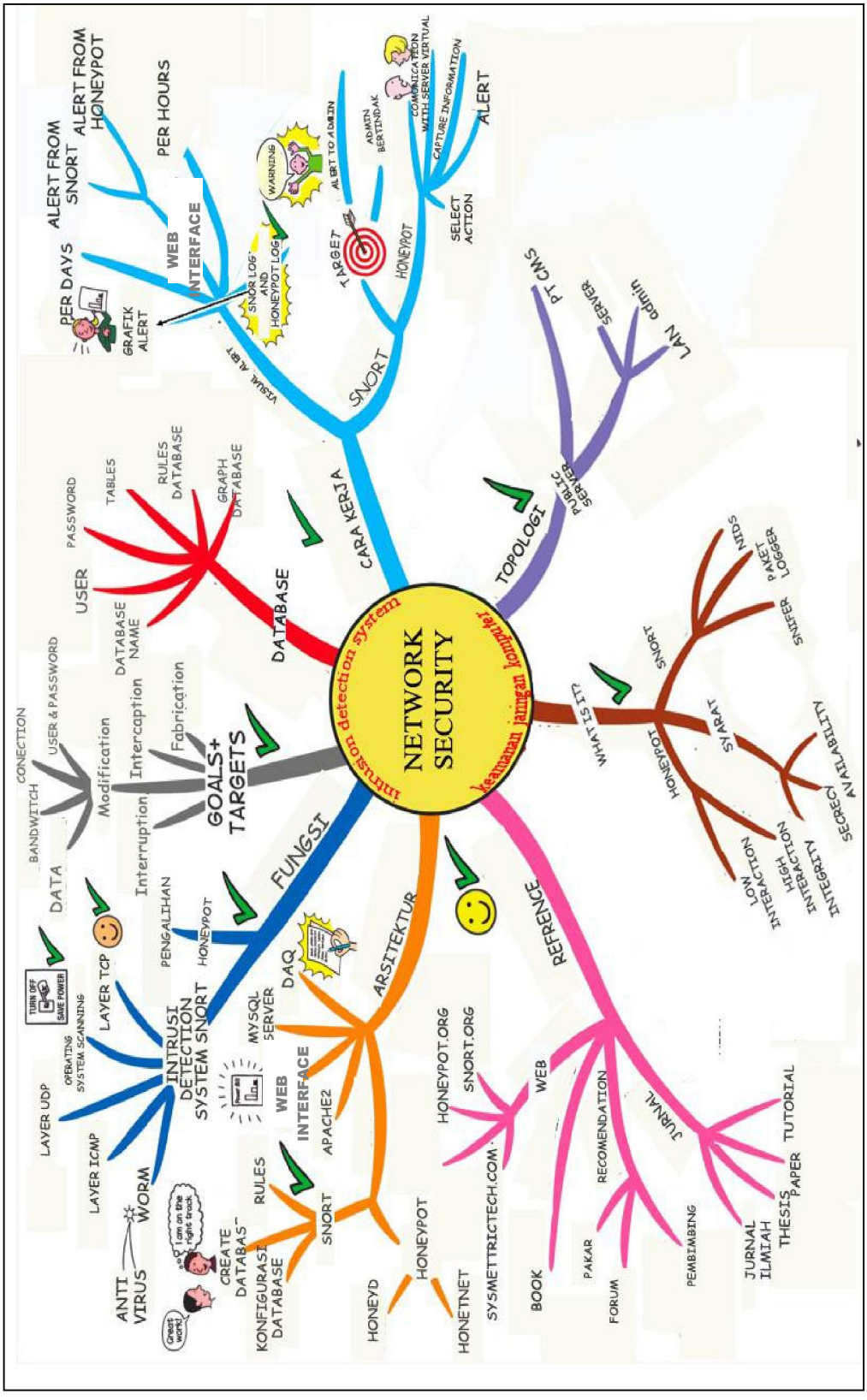
Bab ini menyimpulkan apa yang ada pada bab-bab terdahulu serta memberikan saran atas penulisan tugas akhir ini.

1.7. *Mind Map* Penelitian

Mind map ini bertujuan untuk mempermudah pembaca dalam pemahaman perancangan sistem keamanan yang dibuat dan diteliti, selain itu dengan *mind map* ini dijadikan metode untuk menarik minat pembaca.

Mind map yang dibuat mewakili atau menggambarkan tentang semua aspek yang ada dalam perancangan penelitian.

Berikut *mind map* penelitian yang disusun :



Gambar 1.1 *Mind Map* Penelitian