BAB I

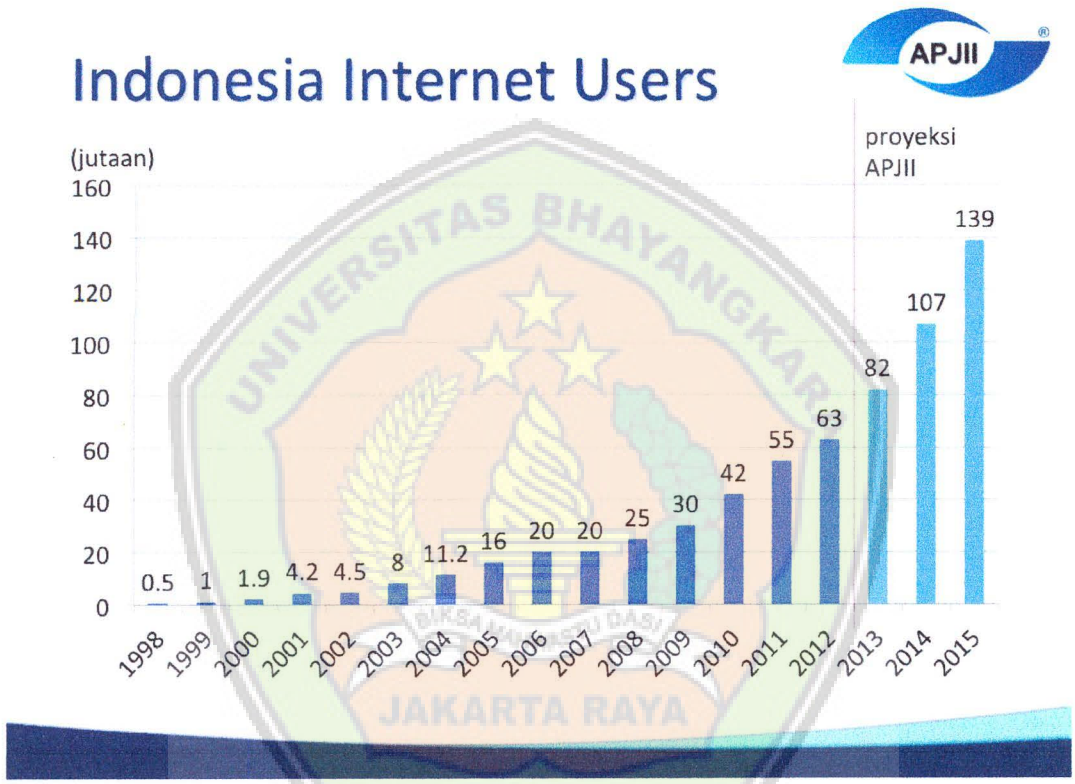
PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Dalam dunia komunikasi data global dan perkembangan teknologi informasi yang senantiasa semakin berkembang pesat. terutama di Indonesia, Sebuah survei yang diselenggarakan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengungkapkan bahwa jumlah pengguna internet di Indonesia tahun 2012 mencapai 63 juta orang atau 24,23 persen dari total populasi negara ini. Tahun depan, angka itu diprediksi naik sekitar 30 persen menjadi 82 juta pengguna dan terus tumbuh menjadi 107 juta pada 2014 dan 139 juta atau 50 persen total populasi pada 2015. Perbandingan pertumbuhan internet Indonesia ini masih sejalan dengan pertumbuhan internet dunia, Indonesia menempati urutan kedelapan di seluruh dunia. Pengguna internet global sendiri, menurut *International Telecommunication Union* (ITU) mencapai angka 2, 421 miliar pada 2011 dari 2, 044 miliar pada tahun sebelumnya.

Perkembangan internet di Indonesia juga diikuti oleh perkembangan peretas. Perlu disadari bahwa untuk mencapai suatu keamanan itu adalah suatu hal yang sangat mustahil, seperti yang ada dalam dunia nyata sekarang ini. Tidak ada satu daerah pun yang betul-betul aman kondisinya, walau penjaga keamanan telah ditempatkan di daerah tersebut, begitu juga dengan keamanan sistem komputer. Namun yang bisa dilakukan adalah untuk

mengurangi gangguan keamanan tersebut. Angka penetrasi internet terhadap populasi menyebar rata disebagian besar wilayah Indonesia. 1,5 juta hacker menyerang internet tiap hari [Rudi Lumanto, Ketua Indonesian Security Incident Response Team on Internet Infrastructure (ID-SIRTII)



Gambar 1.1: Grapik pengguna Internet Di Indonesia
Sumber: http://apjii.or.id

Internet dapat dianggap sebagai mesin yang paling kompleks yang pernah dibangun. Para pengamat IT hampir tidak memahami cara kerjanya, apalagi cara untuk mengamankan (Schneier 2008). Pengenalan teknologi baru seperti perkembangan aplikasi web baru atau meningkatnya penggunaan nirkabel (*Wireless Fidelity*), telah memperburuk fakta ini. *Cybersecurity*, perputaran dari pertumbuhan fenomenal internet, mungkin telah menjadi ancaman yang paling kompleks untuk masyarakat modern. Pengembangan *cybersecurity* telah dikerjakan dan didorong oleh *ingeniosity* dan imajinasi *cyberattackers*. Dalam kata-kata *Carl Landwehr* pada keamanan IEEE (*Institute of Electrical and Electronics Engineers*) dan Privasi (Landwehr 2008), "Pertahanan terdiri dalam memperbaiki saluran pipa". Apa yang kita butuhkan adalah melibatkan *Artificial Intelligence* (AI) dalam *cybersecurity* ". *Cyberspace* adalah infrastruktur yang agak rapuh, tidak dirancang untuk mendukung apa yang dilakukannya saat ini, dan di mana semakin banyak fungsi yang membangun.

Fakta bahwa internet digunakan untuk segala macam kegiatan penting di tingkat individu, perusahaan, organisasi dan bahkan pada tingkat negara telah melakukan segala macam kegiatan berbahaya untuk kerahasiaan data. Serangan maya / *Cyber* terdapat berbagai macam bentuk, Beberapa serangan seperti *Denial of Service* mudah dideteksi. Masalahnya adalah apa yang harus dilakukan terhadap mereka. Bagi

bentuk lain dari serangan, pendeteksian masalah dan kadang-kadang Masalah utamanya.[1]

IDS (Intrusion Detection System) adalah komponen yang penting dalam sebuah jaringan komputer, banyak standar keamanan jaringan pada IDS, apalagi dengan adanya koneksi nirkabel pada sebuah instansi. [2]Penerapan jaringan nirkabel selain memberikan kemudahan dalam berkomunikasi atau transaksi data, ternyata terdapat pula beberapa kelemahan pada segi kemanannya. Jaringan nirkabel tidak memiliki jalur pertahanan yang jelas, sehingga setiap komputer pengguna harus siap terhadap gangguan ataupun serangan yang mungkin terjadi. [3] Masalah tersebut adalah masalah keamanan data yang dikirimkan melalui internet / jaringan lokal. Data yang bisa disebut aman mempunyai 3 sifat, yaitu; *Confidentiality* (Kerahasiaan data), *Integrity* (Keutuhan data) dan *Availability* (Ketersediaan data). Jika data yang telah diproses oleh sistem komputasi tersebut sifatnya kurang dari 3 sifat tersebut, maka tidak ada keamanan pada data tersebut. Sebagai contoh; Data user.dbs yang menyimpan informasi akun user dan password telah di curi / salin, maka sifat '*Confidentiality*' hilang dan data sudah tidak aman lagi. Banyak cara yang dilakukan oleh penyusup dalam aksinya untuk mendapatkan apa yang ia inginkan, termasuk teknik *Social Enginering* yang memanfaatkan *Human Vulnerability*, memanfaatkan celah pada

[1] INTRUSION DETECTION SYSTEMS, Pawel Skrobanek.
[2] Intrusion Detection System, Jack Koziol
[3] Perancangan dan Implementasi Intrusion Detection System pada Jaringan Nirkabel BINUS University

user itu sendiri, mungkin keteledoran dalam perawatan sistem, kurangnya sistem keamanan dan lain-lain.

Banyak cara untuk melakukan pencegahan penyusupan pada sistem jaringan komputer agar sifat-sifat keamanan data tersebut tidak hilang, Salah satunya adalah membangun IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System*). IDS yang artinya adalah Sistem pencegahan penyusup dalam lingkup jaringan komputer yang bersifat lokal. Sedangkan IPS adalah Sistem Pencegahan Penyusup dalam sistem jaringan komputer lokal maupun interlokal.

Permasalahan yang terjadi di CV. Cyber Makassar Development ini pernah terjadi exploitasi data, termasuk software yang telah di develop oleh karyawan yang bekerja di CV. Cyber Makassar ini. Estimasi terjadinya eksploitasi dikarenakan CV ini mempunyai jaringan nirkabel gratis yang dapat diakses orang luar disekitarnya, tidak menutup kemungkinan terjadinya serangan ini lewat jaringan nirkabel tersebut. Menurut data yang didapat, semenjak CV ini berdiri sudah 2 kali terjadi eksploitasi komputer. Tepatnya pada tanggal 02 Januari 2013 dan tanggal 12 Januari 2013, kerugian yang ditimbulkan berkisar antara 10 jutaan karena *source code* akan dijual tersebar bebas di *search engine.*

Maka dari ini semua, IDS memang diperlukan di sistem jaringan komputer pada CV. Cyber Makassar Development demi terjaganya data-data penting dan software yang akan di jual.

1.2 IDENTIFIKASI MASALAH

Dalam penulisan skripsi ini, penulis mengidentifkasikan masalah yang ada pada sistem deteksi intrusi sebagai berikut;

1. Belum adanya sistem keamanan jaringan di CV. Cyber Makassar Development
2. Belum mempunyai sistem pemantauan keluar masuk traffic data pada jaringan di CV. Cyber Makassar sehingga berpotensi adanya penyusupan berupa malware maupun backdoor yang dibuat untuk mencuri data.
3. Pernah terjadi eksploitasi pada komputer owner yang membuat aplikasi-aplikasi development dicuri oleh *hacker* pada tanggal 02 Januari 2013 dan 12 Januari 2013.

1.3 PERUMUSAN MASALAH

Berdasarkan tema dan latar belakang masalah yang telah diuraikan diatas, maka dirumuskan masalah sebagai berikut;

1. Bagaimana membangun keamanan Jaringan dengan IDS.
2. Bagaimana membuat sistem pemantau traffic keluar masuk pada jaringan komputer di CV. Cyber Makassar Development.
3. Bagaimana pencegahan khususnya untuk menangani dan menangkal eksploitasi.

1.4 BATASAN MASALAH

Batasan masalah yang dapat diambil dari tema ini adalah;

1. Pengamanan jaringan komputer hanya dalam ruang lingkup NIDPS saja.
2. Keamanan jaringan komputer berbasis NIDPS ini dibangun pada jaringan komputer CV. Cyber Makassar Development.

1.5 TUJUAN DAN MANFAAT PENELITIAN

Hasil penelitian ini diharapkan dapat digunakan sebagai langkah awal untuk membangun sistem keamanan jaringan yang terpantau secara real-time oleh administrator jaringan dan meminimalisir serangan-serangan yang bertujuan merugikan pihak CV. Cyber Makassar Development.

1.6 METODE PENELITIAN

Metode yang akan digunakan dalam penelitian ini terdiri dari langkah-langkah berikut:

1. Metode Observasi
   a. Melakukan observasi terhadap sistem jaringan komputer pada Mr. Montir Mutiara Grande Tambun Utara.
   b. Konfigurasi sistem keamanan jaringan dengan program-program yang berfungsi sebagai NIDS.

c. Melakukan simulasi hacking bertujuan untuk mencari *bug* atau celah keamanan IDS ini.

2. Studi Pustaka

Melakukan studi kepustakaan dari berbagai referensi yang berkaitan dengan penelitian yang dilakukan. Topik-topik yang akan dikaji antara lain meliputi: pengenalan IDS, Snort, percobaan penetrasi pada jaringan yang telah terpasang IDS beserta simulasinya.

3. Metode Wawancara

Dalam metode ini penulis bertatap muka dengan pihak-pihak yang terkait di CV. Cyber Makassar Development untuk menanyakan hal-hal yang berhubungan dengan penyusunan skripsi ini.

1.7 SISTEMATIKA PENULISAN

Dalam penulisan skripsi ini mempunyai sistematika penulisan adalah sebagai berikut :

BAB I PENDAHULUAN

Dalam bab ini akan diuraikan mengenai latar belakang masalah, identifikasi masalah, batasan masalah, maksud dan tujuan penulisan, metode penelitian yang digunakan dalam pengumpulan data serta sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab ini penulis menjelaskan tentang landasan-landasan teori yang berkaitan dengan topik pembahasan, diantaranya konsep dasar sistem, konsep dasar IDS, Konsep dasar jaringan, pengembangan sistem, analisa sistem, perancangan sistem, peralatan pendukung seperti : UML bagan alur (*Flowchart*), spesifikasi proses, bagan terstruktur, spesifikasi modul, Selain itu juga menerangkan deskripsi tentang program atau tool intrusi.

BAB III ANALISA SISTEM BERJALAN

Dalam bab ini berisi tentang topologi jaringan pada umumnya, UML, spesifikasi proses, analisa masukan dan keluaran,. Pada bab ini juga dibahas tentang pokok permasalahan yang dihadapi dan alternatif pemecahannya.

BAB IV RANCANGAN SISTEM USULAN

Dalam bab ini menjelaskan tentang proses rancangan sistem deteksi intrusi yang berupa Topologi jaringan yang sudah ada IDS, penjelasan *tool*, bagan terstruktur, spesifikasi modul, rancangan masukan dan rancangan keluaran, implementasi.

BAB V KESIMPULAN DAN SARAN

Diakhir bab ini menjelaskan tentang kesimpulan dari penulisan skripsi yang telah dibuat dan penulis memberikan saran-saran yang sekiranya dapat bermanfaat bagi pembaca.