Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

Team project ©2017
Dony Pratidana S. Hum | Bima Agus Setyawan S. IIP

Bab I

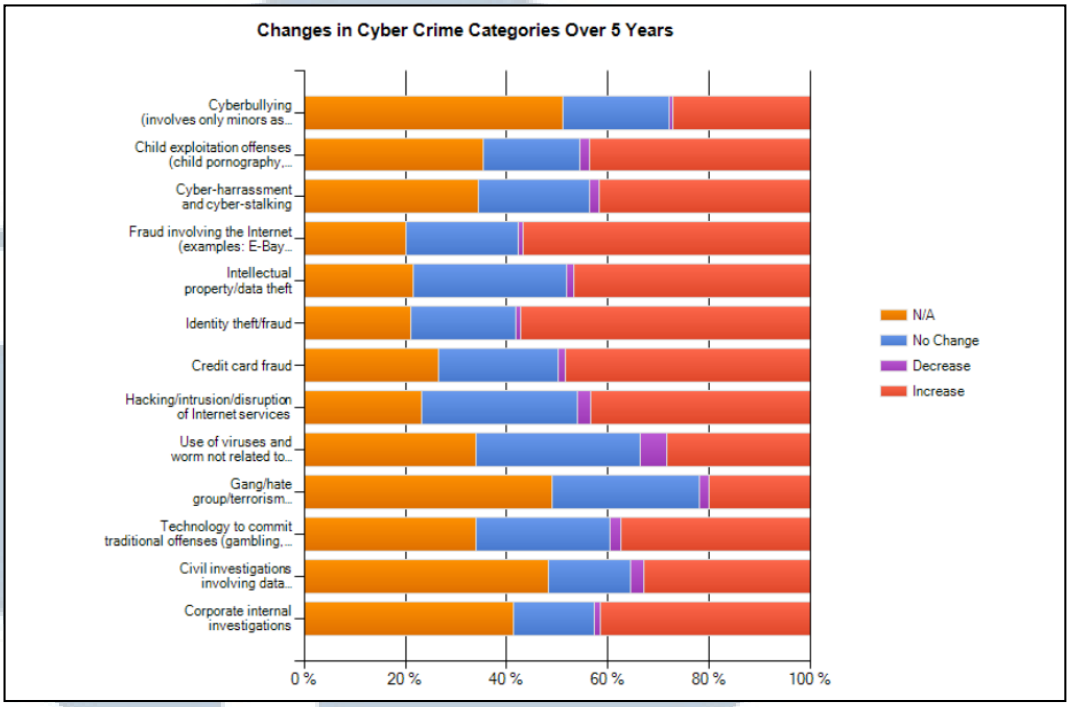
Pendahuluan

1.1 Latar Belakang

Dalam lima tahun terakhir, kejahatan *cyber* semakin meningkat [1]. Baik dalam kasus pencurian identitas, virus, maupun penyusupan (*intrusion*) ke sebuah sistem. Seperti yang terpampang di grafik pada gambar 1. Grafik tersebut menggambarkan hasil survei yang dilakukan oleh *High Tech Crime Investigation Association* (HTCIA) tentang perubahan jumlah kasus kejahatan *cyber* dalam 5 tahun terakhir [1]. Salah satu kejahatan *cyber* yang dapat ditangani dengan bantuan *software* adalah kejahatan *hacking, intrusion,* dan *disruption* yaitu dengan menggunakan *software Intrusion Detection System* yang digunakan dalam *Intrusion Prevention System.* Sekitar 45% responden menyatakan bahwa kejahatan pada sektor tersebut meningkat dalam 5 tahun terakhir. Salah satu IDS yang berperan aktif dalam mendeteksi kejahatan *cyber* tersebut adalah Snort.

Snort [2] adalah salah satu perangkat lunak *Network-Based* IDS (*Intrusion Detection Software*) yang terkemuka di dunia. Hampir empat ratus ribu pengguna IDS menggunakan *software* tersebut [2]. Namun, Snort tidak menyediakan GUI(*Grafical User Interface*) yang memadai. Untuk mendapatkan GUI yang lebih baik, *user* harus menginstall apikasi tersendiri. Salah satu aplikasi antar muka pelaporan Snort yang memiliki banyak fitur adalah BASE [3].

Pengembangan Sistem Pelaporan..., Bagas Adi Wicaksono, FTI UMN, 2012



Gambar 1. Grafik Perubahan Jumlah Kasus Kejahatan *cyber* [1]

BASE [4] menampilkan informasi berupa *log* dan statistik dari Snort pada sebuah halaman web. Ketika Snort menemukan adanya suatu *incident*, Snort akan mengirim sinyal *alert* yang dilanjutkan dengan menyimpan detail serangan ke database. Database inilah yang akan ditampilkan ketika pengguna/admin *log*in ke halaman BASE. Menurut artikel yang diterbitkan James Lay [3], BASE merupakan salah satu dari empat GUI yang banyak digunakan sebagai antarmuka dari Snort. Selain itu, BASE memiliki fitur paling lengkap dan *dependencies* yang paling sedikit dari tiga pesaingnya [3].

Alert yang ada pada IDS bertujuan untuk memberitahu *system administrator* bahwa ada serangan pada sistemnya [5]. Namun, Sistem seperti di atas tidak memungkinkan pengguna mengetahui adanya serangan secara langsung

(*real time*), sehingga admin tidak bisa mengambil tindakan yang diperlukan secara langsung. Maka dari itu dibutuhkan suatu sistem pelaporan yang mendukung *real time notification*. Untuk mendukung kerja dari sistem administrator, sistem pelaporan yang ada harus bisa memberi laporan yang ringkas dan padat sesuai dengan permintaan *user* [6].

Di sisi lain, penggunaan *Instant Messenger* terus bertambah. Tak hanya digunakan di *desktop*, *Instant Messenger* telah menjadi *trend* di perangkat *mobile*. Bahkan *Instant Messaging* diproyeksikan bakal menggantikan SMS sebagai media komunikasi *text* [7].

Dewasa ini, *Instant Messenger* juga digunakan di banyak platform sebagai *real time notification* [8]. Di samping itu, IM dapat menyediakan fasilitas *query* yang tidak bisa diterapkan secara mudah di media komunikasi lainnya[8]. Dengan *query* yang bisa diterapkan dalam *Instant Messenger, System Administrator* bisa berinteraksi dengan sistemnya untuk mendapatkan status maupun kondisi sistem yang diinginkannya [9].

Tidak seperti SMS *gateway*, *Instant Messenger* hanya membutuhkan koneksi internet untuk tersambung ke server. Sedangkan, SMS *gateway* membutuhkan biaya setiap kali mengirim suatu pesan sehingga akan membutuhkan biaya yang tidak sedikit jika SMS *gateway* diterapkan dalam sebuah sistem *notification*. Sehingga biaya yang dikeluarkan apabila menggunakan *Instant Messenger* jauh lebih sedikit [8].

Yahoo! Messenger adalah salah satu protokol *instant messenger* yang banyak digunakan (sekitar 22.000.000 pengguna) [10]. Yahoo! Messenger dapat

Pengembangan Sistem Pelaporan..., Bagas Adi Wicaksono, FTI UMN, 2012

digunakan pada tiga macam Sistem Operasi *mobile* terbesar saat ini yaitu BBOS [11], iOS [12], dan Android [13]. Selain itu, banyak aplikasi IM yang menyediakan layanan Yahoo! Messenger tersebut seperti eBuddy [14] dan Nimbuzz [15]. Maka dari itu, *messenger* tersebut dapat dikatakan dapat digunakan pada semua *platform*.

Penelitian ini memanfaatkan *Instant Messenger* sebagai sistem pelaporan dinamis dengan fasilitas *real-time notification* pada aplikasi *Intrusion Detection System.* Sehingga pengguna Snort dapat memperoleh *alert* Snort secara *real-time*.

1.2 Batasan Masalah

Batasan masalah penelitian ini adalah

1. *operating system* yang digunakan adalah Linux (CentOS 6.0),
2. *software* IDS yang digunakan adalah Snort 2.9.1.2, dan
3. penyajian laporan secara dinamis atas masukan dari pengguna menggunakan teknologi *instant messenger* Yahoo! Messenger sebagai perantara.

1.3 Rumusan Masalah

Masalah yang ingin diatasi pada penelitian ini adalah

- Bagaimana mengembangkan sistem *notification* IDS yang *real-time*?
- Bagaimana membuat sistem pelaporan yang bisa diakses secara *mobile*?

UNIVERSITAS MULTIMEDIA NUSANTARA

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menerapkan teknologi *Instant Messenger* sebagai sistem pelaporan dengan fasilitas *real-time notification* pada aplikasi *Intrusion Detection System.*

1.5 Manfaat Penelitian

Manfaat yang dapat diperoleh setelah diadakan penelitian ini:

- Membantu pengguna/*system administrator* dalam mengetahui dan menggali informasi tentang serangan pada sistem secara *real-time* serta menindaklanjuti *incident* yang terjadi.
- Memfasilitasi sistem perlindungan yang sudah ada tanpa menambah biaya yang relatif besar dibandingkan dengan metode SMS *Gateway*. Karena dengan metode ini, pengguna hanya membutuhkan biaya internet sedangkan dengan SMS *Gateway* pengguna harus menyediakan biaya untuk setiap pesan yang dikirim.
- Memungkinkan pengguna dapat memonitor sistem mereka di mana saja menggunakan teknologi *mobile instant messenger*.

UNIVERSITAS
MULTIMEDIA
NUSANTARA