RINGKASAN

YANDRA PERMI PUTRA. Implementasi *Intrusion Prevention System* Menggunakan Snort di Lab *Development* BPPT. *Implementation of Intrusion Prevention System Using Snort at BPPT Development Lab*. Dibimbing oleh RINGGA GILANG BASKORO.

BPPT memegang peranan penting dalam hal pengkajian dan penerapan teknologi. BPPT terdapat Pusat Teknologi Informasi dan Komunikasi (PTIK). Di PTIK terdapat Lab *Development* yang fungsinya memegang peranan penting untuk menjaga stabilitas jaringan serta mengelola data-data yang terdapat pada server BPPT. Untuk menjaga data-data tersebut sistem keamanan di Lab *Development* BPPT hanya dapat mendeteksi serangan yang masuk tetapi tidak dapat mencegah terjadinya serangan, oleh karena itu diperlukan perimeter yang dapat melakukan pencegahan dari serangan hacking yang berbasis *open source* khususnya di Lab *Development* BPPT. Untuk menjawab permasalahan tersebut dibuatlah Implementasi *Intrusion Prevention System* Menggunakan Snort di Lab *Development* BPPT. *Intrusion Prevention System* (IPS) disini merupakan sebuah sistem yang dapat mencegah serangan dari peretas dan dapat melakukan monitoring keamanan jaringan.

Pembuatan Implementasi *Intrusion Prevention System* Menggunakan Snort di Lab *Development* BPPT menggunakan beberapa metode. Metode yang digunakan dalam implementasi *intrusion prevention system* terdiri dari tahap analisis, perancangan, implementasi dan pengujian. Pembuatan sistem ini sebagai solusi untuk mencegah terjadinya serangan pada sistem jaringan di Lab *Development* BPPT agar jaringan di BPPT menjadi aman dan data-data penting yang terdapat pada server menjadi terjaga sehingga dalam proses pengkajian dan penerapan teknologi bisa berjalan sebagaimana mestiya. Perangkat lunak yang digunakan sebagai *intrusion prevention system* pada sistem ini adalah Snort. Untuk menerapkan *intrusion prevention system* pada Snort dibutuhkan *Data AcQusition* (DAQ). DAQ disini berfungsi untuk mengaktifkan semua fitur dari Snort. DAQ yang digunakan pada sistem ini adalah *NetFilter-queue* (NFQ), NFQ disini berfungsi mengalihkan segala paket ke dalam Iptables. Paket tersebut akan ditindaklanjuti oleh Snort. Jika Snort telah dijalankan maka Snort menghasilkan sebuah log yang nantinya log tersebut akan dihubungkan dengan basis data dengan bantuan barnyard2 dan untuk menampilkan hasil serangan ditampilkan menggunakan BASE.

Kata Kunci: *Data AcQusition*, *Intrusion Prevention System*, Snort.