RINGKASAN

KRI IRMAN SYAH. Implementasi *Instrusion Prevention System* (IPS) enggunakan Snort dengan NFQ di DISKOMINFOSTANDI Kota Bogor *trusion Prevention System (IPS) Implementation Uses Snort with NFQ at skominfostandi Bogor*). Dibimbing oleh ARIF HARBANI.

Diskominfostandi merupakan penyelenggara jasa internet untuk instansi merintahan Kota Bogor. Diskominfostandi juga menyediakan *server* bagi tansi Pemerintahan Kota Bogor yang membutuhkan. *Server-server* tersebut ring mengalami permasalahan, seperti : *server down* atau *server* diretas. Hal ini luga terjadi akibat ulah dari peretas. Untuk mengantisipasi hal tersebut buatlah percobaan mengenai *Intrusion Prevention System* (IPS) Menggunakan ort dengan NFQ di Diskominfostandi Kota Bogor. IPS adalah sistem yang pat memblokir percobaan serangan dari peretas dan dapat memantau keamanan ingan. Salah satu perangkat lunak yang dapat menerapkan IPS adalah Snort. tuk menerapkan IPS pada Snort dibutuhkan *Data AcQusition* (DAQ). DAQ alah *library* keluar masuknya paket. Salah satu DAQ yang dapat digunakan alah *NetFilter-queue* (NFQ). NFQ adalah *target* dari *Netfiilter* atau Iptables ng berfungsi untuk mengalihkan setiap paket ke dalam antrian. Paket tersebut an ditindaklanjuti oleh Snort.

Percobaan penerapan IPS di Diskominfostandi dilakukan dengan 4 metode u tahap. Metode pertama adalah metode analisis. Metode analisis dilakukan ngan cara mengidentifikasi dan menganalisis masalah jaringan yang ada di skominfostandi, yaitu masalah keamanan jaringan dan kebutuhan yang perlukan untuk membuat sistem IPS dalam mengatasi masalah tersebut. Metode dua adalah metode perancangan. Pada metode ini dibuat rancangan atau konsep r sistem yang merujuk pada kebutuhan dari tahap analisis dan dibuat topologi ingan yang merujuk pada topologi yang ada di Diskominfostandi. Metode ke a yaitu metode implementasi, yang meliputi penginstalasian dan ngonfigurasian perangkat lunak yang dibutuhkan, seperti : Snort, DAQ, dan n-lain. Metode ke empat yaitu metode pengujian. Pada metode ini, sistem ujicoba dengan beberapa pengujian, diantaranya adalah percobaan SSH dan angan DoS *SYNflood*.

Hasil percobaan menunjukkan sistem IPS yang diimplementasikan berhasil mblokir percobaan SSH dan serangan DoS *SYNflood* yang dilakukan pada ap pengujian. Pengembangan sistem perlu ditingkatkan agar sistem IPS njadi sistem pengaman jaringan yang lebih sempurna.

ta kunci: *Instrusion Prevention System*, Snort, *Data AcQusition*, *NetFilter-eue*,