



RINGKASAN

KRI IRMAN SYAH. Implementasi *Intrusion Prevention System* (IPS) menggunakan Snort dengan NFQ di DISKOMINFOSTANDI Kota Bogor (*Intrusion Prevention System (IPS) Implementation Uses Snort with NFQ at Diskominfostandi Bogor*). Dibimbing oleh ARIF HARBANI.

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

Percobaan penerapan IPS di Diskominfostandi dilakukan dengan 4 metode atau tahap. Metode pertama adalah metode analisis. Metode analisis dilakukan dengan cara mengidentifikasi dan menganalisis masalah jaringan yang ada di diskominfostandi, yaitu masalah keamanan jaringan dan kebutuhan yang diperlukan untuk membuat sistem IPS dalam mengatasi masalah tersebut. Metode kedua adalah metode perancangan. Pada metode ini dibuat rancangan atau konsep sistem yang merujuk pada kebutuhan dari tahap analisis dan dibuat topologi jaringan yang merujuk pada topologi yang ada di Diskominfostandi. Metode ketiga yaitu metode implementasi, yang meliputi penginstalasian dan konfigurasi perangkat lunak yang dibutuhkan, seperti : Snort, DAQ, dan lain-lain. Metode keempat yaitu metode pengujian. Pada metode ini, sistem diujicoba dengan beberapa pengujian, diantaranya adalah percobaan SSH dan serangan DoS *SYNflood*.

Hasil percobaan menunjukkan sistem IPS yang diimplementasikan berhasil memblokir percobaan SSH dan serangan DoS *SYNflood* yang dilakukan pada tahap pengujian. Pengembangan sistem perlu ditingkatkan agar sistem IPS menjadi sistem pengamanan jaringan yang lebih sempurna.

Kata kunci: *Intrusion Prevention System*, Snort, *Data Acquisition*, *NetFilter-queue*,

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB.
2. Dilarang mempublikasikan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB.

