1. Pendahuluan

Latar Belakang

Penggunaan teknologi informasi terus meningkat dari waktu ke waktu, yang hal ini berarti juga turut meningkatkan pemanfaatan jaringan internet oleh masyarakat baik untuk pencarian informasi, kolaborasi, komunikasi jarak jauh, ataupun untuk menikmati hiburan. Namun, pemanfaatan teknologi informasi dan juga internet sering kali disalahgunakan oleh beberapa pihak yang ingin mengambil keuntungan dengan cara melakukan tindakan kejahatan seperti kejahatan *cyber*. Tidak hanya perusahaan besar yang menjadi target kejahatan, tetapi *home network* pun seringkali menjadi target kejahatan [1] [2].

Jumlah perangkat yang terhubung ke *home network* semakin lama semakin meningkat, terlebih dengan munculnya produk-produk yang pintar seperti tv pintar, speaker pintar, serta IoT untuk rumah pintar [2]. Perangkat-perangkat tersebut terkadang didesain tidak dengan baik dari sisi keamanan, padahal bisa jadi memiliki sensitifitas yang tinggi terkait dengan informasi pribadi. Hal ini medapat menimbulkan potensi diserang melalui jaringan yang terhubung ke *home network* tersebut seperti melalui internet [2].

Atas dasar alasan tersebut, diperlukan sebuah perangkat yang dapat mengontrol perangkat-perangkat pintar tersebut, termasuk mengontrol aliran data yang masuk dan keluar dari jaringan lokal. Perangkat ini tidak boleh mengonsumsi daya yang besar karena perangkat rumahan (atau non-korporasi) yang biasa digunakan sehari-hari salah satu tuntutan desainnya adalah berdaya rendah. Namun, perangkat ini juga harus tidak membuat keterlambatan dalam aliran data, sekaligus mempunyai kemampuan penyaringan paket yang relatif baik [2].

Perangkat yanmg memenuhi spesifikasi yang disebutkan di atas, dan relative popular digunakan adalah *Single Board Computer* (SBC). Salah satu SBC yang relative popular dan dapat digunakan adalah *Raspberry Pi* [2].

Untuk menciptakan keamanan pada jaringan, termasuk pada *home network*, dibutuhkan sebuah pendeteksi yang akan membantu pengguna untuk menyadari bahwa terdapat serangan [2]. IDS (Intrusion Detection System) dapat diimplementasikan untuk mendeteksi adanya sebuah serangan, termasuk mendeteksi aktivitas yang mencurigakan karena IDS berfungsi memonitoring jaringan secara *real-time* [1]. Terdapat berbagai *tools* IDS (Intrusion Detection System) yang umum digunakan yaitu *Snort*, Suricata dan Bro IDS [3].

Dengan keterbatasan komputasi dari *Raspberry Pi*, pemilihan *Snort* sebagai IDS relatif beralasan karena dibanding dengan Bro, *Snort* lebih mampu menekan tingkat *load* dari CPU, akan tetapi kekurangan kedua *tools* ini adalah *packet loss* yang dihasilkan tinggi [4].

Untuk mengatasi masalah tersebut pada *Snort*, digunakan PF_RING agar *packet capture* yang mampu ditangkap dapat ditingkatkan [5].

Topik dan Batasannya

Topik yang dibahas pada penelitian ini adalah bagaimana mengimplementasikan PF_RING pada *Snort* IDS untuk mengomptimalkan kinerja paket *capture* pada saat sistem diserang. Dalam penelitian ini, serangan yang digunakan yaitu DoS.

Tujuan

Membangun sistem yang dapat mendeteksi serangan dan memaksimalkan paket *capture* pada sistem terutama pada saat sistem diserang. Dimana hasil dari sistem berupa alert jika terdapat serangan dan persentase *packet capture* dengan PF_RING lebih maksimal.

Organisasi Tulisan

Pada bab dua, jurnal ini akan menjelaskan studi terkait yang berisi mengenai teori yang mendukung penelitian ini. Pada bab tiga menjelaskan mengenai rancangan sistem yang dibangun. Pada bab keempat akan menjelaskan mengenai pengujian dan analisis dari penelitian yang dilakukan. Pada bab lima akan menjelaskan mengenai kesimpulan dari penelitian dan saran untuk penelitian selanjutnya.